

---

# Electronic Warfare

---



---

U.S. Marine Corps

DEPARTMENT OF THE NAVY  
Headquarters United States Marine Corps  
Washington, DC 20380-0001

20 May 1991

FOREWORD

1. PURPOSE

Fleet Marine Force Manual (FMFM) 7-12, *Electronic Warfare*, establishes doctrine for employment and use of electronic warfare in support of the Marine Air-Ground Task Force (MAGTF).

2. SCOPE

This manual presents a detailed account of electronic warfare doctrine, tasks, and structure in MAGTF and joint/combined operations, specifically for personnel who work within the field of electronic warfare.

3. SUPERSESSION

Operational Handbook (OH) 7-12, *Electronic Warfare*, dated October 1986.

4. CHANGES

Recommendations for improving this manual are invited from commands as well as directly from individuals. Forward suggestions using the User Suggestion Form format to—

Commanding General  
Marine Corps Combat Development Command (WF 12)  
Quantico, Virginia 22134-5010

5. CERTIFICATION

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS



M. P. CAULFIELD  
Major General, U.S. Marine Corps  
Deputy Commander for Warfighting  
Marine Corps Combat Development Command  
Quantico, Virginia

DISTRIBUTION: 13900057300

## USER SUGGESTION FORM

From:

To: Commanding General, Marine Corps Combat Development Command (WF 12), Quantico,  
Virginia 22134-5010

Subj: RECOMMENDATIONS CONCERNING FMFM 7-12, *ELECTRONIC WARFARE*

1. In accordance with the Foreword to FMFM 7-12, which invites individuals to submit suggestions concerning this FMFM directly to the above addressee, the following unclassified recommendation is forwarded:

<u>Page</u>	<u>Article/Paragraph No.</u>	<u>Line No.</u>	<u>Figure/Table No.</u>	
Nature of Change:	<input type="checkbox"/> Add	<input type="checkbox"/> Delete	<input type="checkbox"/> Change	<input type="checkbox"/> Correct

2. Proposed new verbatim text: (Verbatim, double-spaced; continue on additional pages as necessary.)

3. Justification/source: (Need not be double-spaced.)

NOTE: Only one recommendation per page.

Record of Changes

Change No.	Date of Change	Date of Entry	Organization	Signature

# Electronic Warfare

## Table of Contents

### Chapter 1. Introduction

Paragraph		Page
1001	Doctrine, Tactics, Techniques, and Procedures	1-1
1002	Structure of MAGTFs	1-2
1003	Training	1-3
1004	Standing Operating Procedures	1-3
1005	Signals Intelligence	1-3
1006	Signal Security	1-3

### Chapter 2. Electronic Warfare Doctrine

2001	General	2-1
2002	Electronic Warfare Support Measures	2-2
2003	Electronic Countermeasures	2-3
2004	Electronic Counter-Countermeasures	2-7
2005	Communications	2-8
2006	Authority of Commanders and Their Staffs	2-8
2007	Control and Coordination	2-9
2008	Ground Electronic Warfare	2-10
2009	Airborne Electronic Warfare	2-11
2010	Electronic Warfare in Various Types of Operations	2-12

### Chapter 3. Electronic Warfare Resources

3001	General	3-1
3002	Radio Battalion	3-1
3003	Marine Tactical Electronic Warfare Squadron	3-1
3004	Other Services	3-2
3005	National Level Agencies	3-2
3006	Duties of Personnel	3-3
3007	Signals Intelligence/Electronic Warfare Coordination Center	3-4

Paragraph		Page
<b>Chapter 4.</b>	<b>Electronic Warfare Planning</b>	
4001	General	4-1
4002	ESM Plans	4-1
4003	ECM Plans	4-1
<b>Chapter 5.</b>	<b>Electronic Warfare Coordination and Control</b>	
5001	General	5-1
5002	Command and Support Relationships	5-1
5003	Authority of Area Commander	5-3
5004	Tasking Authority	5-4
5005	Coordination of EW	5-4
5006	Tasking of MAGTF Assets	5-4
5007	Requests for External Signals Intelligence, EW, and SI Support	5-5
<b>Chapter 6.</b>	<b>Electronic Counter-Countermeasures Techniques</b>	
6001	General	6-1
6002	Preventive ECCM	6-1
6003	Remedial ECCM	6-3
<b>Chapter 7.</b>	<b>Electronic Warfare Reports</b>	
7001	General	7-1
7002	MIJI Reports	7-1
7003	TERPES-Generated Reports	7-1
<b>Chapter 8.</b>	<b>Employment of MAGTF Electronic Warfare Units With the Ground Combat Element</b>	
8001	General	8-1
8002	Planning Considerations	8-1
8003	Employment Considerations	8-1
8004	Concepts of Employment	8-2
<b>Chapter 9.</b>	<b>Electronic Warfare in Amphibious Operations</b>	
9001	Amphibious Operations Phases	9-1
9002	Responsibilities	9-2
9003	Tasks During Planning	9-3
9004	Planning Considerations	9-3
9005	Phasing of Electronic Warfare Personnel Ashore	9-3

Paragraph		Page
<b>Chapter 10.</b>	<b>Electronic Threat</b>	
10001	General	10-1
10002	Concepts	10-1
10003	Electronic Countermeasures Threat	10-1
10004	Electronic Warfare Capabilities	10-2
10005	Tactical Reconnaissance	10-2
10006	Radioelectronic Combat	10-3
10007	Complementary Roles of RDF and Intercept	10-5
10008	Complementary Roles of RDF and ECM	10-6
<b>Appendixes:</b>		
A	Graphic Formats and Color Coding	A-1
B	Joint Tactical Electronic Warfare Request Form	B-1
C	Electronic Jamming	C-1
D	Electronic Deception	D-1
E	Communication ECCM Training	E-1
F	Electronic Warfare Appendix Format	F-1
G	Frequency Band Designations	G-1
H	Glossary	H-1
I	References	I-1
<b>Index</b>		<b>Index-1</b>

## PREFACE

Electronic warfare is almost as old as the radio. For more than 80 years military forces have conducted electronic warfare. One would think that an area of warfare would be well understood after that length of time. Yet for many, electronic warfare remains a black art, a deep secret, something done behind green doors. While many of the *details* of electronic warfare operations are classified, the *basics* of electronic warfare are unclassified and easy to understand. The *details* must remain classified because success in many electronic warfare operations depends upon the enemy being complacent and not taking all the precautions possible to protect his radio communications and other electronic emissions from intercept and analysis by our electronic warfare agencies. If the enemy knows what we know about his radio communications and other electronic emissions, his complacency is usually destroyed and he quickly takes those measures necessary to protect his radio communications and other electronic emissions from our collection and analysis efforts. What we know about an enemy's radio communications and other electronic emissions is highly classified to keep the enemy complacent. Those of us who are not directly involved in signals intelligence, electronic warfare support measures, and electronic countermeasures can make electronic warfare work for us if we understand the basics of electronic warfare explained in this manual.

This preface is an introduction to electronic warfare for those who view electronic warfare as a great mystery. The three stories related below are intended to give the reader a taste of what electronic warfare is and how they can use it to help themselves. These stories do not tell all that one should know about electronic warfare. For that, the reader must also read the numbered chapters and the appendixes in this manual, other manuals on electronic warfare, and the history of electronic warfare.

The first recorded use of electronic warfare in combat occurred during the Russo-Japanese War. On an early April morning in 1904, two Japanese armored cruisers were bombarding the Russian naval base at Port Arthur. Smaller ships, using radios, were spotting the fall of shells and passing corrections to the cruisers. Ashore, a Russian radio operator heard the Japanese signals and, realizing their importance, continually keyed his transmitter to jam them. As a result, the Japanese shells fell short of their targets and little damage was done. Electronic countermeasures (ECM) had been born.

The next example falls in the category of signals intelligence/electronic warfare support measures. In the spring of 1942 the American Navy was rebuilding while attempting to hold the line in the Pacific War. At the Battle of the Coral Sea, the American Navy was finally able to check a Japanese offensive, but at a cost in aircraft carriers it could ill afford. Admiral Nimitz knew the Japanese would attack again. Because the Japanese still had a significant numerical advantage, American naval strength could only be committed at the decisive place and time. In late May, Japanese Admiral Yamamoto launched an offensive toward Midway Island with a feint at the Aleutians. At this critical juncture, American Naval Intelligence

electronically intercepted and exploited Japanese message traffic which provided not only Yamamoto's principal objective, but also order of battle information which allowed Nimitz to accurately assess the tactical situation. Based on that assessment, Admiral Nimitz made his decision to take the calculated risk of engaging the Japanese Navy near Midway. That battle is frequently credited with turning the tide in the Pacific War. The resulting decisive defeat of the Japanese was brought about through the skill, courage, and dedication of the sailors and naval aviators who participated. But that skill, courage, and dedication would have gone for naught had the American forces not been at the critical point at the critical time. It was the American electronic warfare success that made that possible, thereby making a significant contribution to final victory.

The final area of electronic warfare to consider is electronic counter-countermeasures (ECCM). The need to deny the enemy knowledge of friendly activity through passive security means has always been important. Electronic security is an extension of old requirements to new technology. ECCM has been essential to overall operations security since the military started using radios. In late 1944, the Allies were surprised by the German offensive now known as the Battle of the Bulge. This offensive was a surprise simply because the Germans kept all mention of the offensive off any radio circuits until the attack started.

These examples indicate the importance of electronic warfare. The remainder of this publication will give you an idea how to use the concepts of electronic warfare to improve your chance for battlefield success.

# Chapter 1

## Introduction

### 1001. Doctrine, Tactics, Techniques, and Procedures

**a.** This manual provides general guidance (doctrine and tactics) and specific guidance (techniques and procedures). It is important to understand the difference between these types of guidance and their applicability. Guidance on the conduct of combat operations varies from the very general to the very specific. Usually, the more general the guidance, the more widely applicable it is; and the more specific the guidance, the fewer the number of situations in which it can be applied. The most general guidance is called doctrine, while procedures are the most specific guidance. Tactics and techniques fall between doctrine and procedures, with tactics being more general than techniques. (See fig. 1-1.)

**(1) Doctrine.** Fundamental principles by which the military forces guide their actions in support of objectives. It is authoritative but requires judgment in application. (Joint Pub 1-02.) Doctrine is a collection of words which describes how military organizations function and how military operations are conducted.

Each principle has (1) a word or phrase for a name and (2) a definition which explains or describes the principle. The definition may include a list of functions or a list of parts. Doctrine is important because words are the tools for thinking, teaching, and giving directions. A person's understanding of what is happening around him can only be as precise as the words he uses to describe and think about it; the instructions, whether in the classroom or on the battlefield, can be only as precise as the words available to give those instructions.

**(2) Tactics.** 1. The employment of units in combat. 2. The ordered arrangement and maneuver of units in relation to each other and/or to the enemy in order to use their full potentialities. (Joint Pub 1-02.) (Example: The placing of radio antennas so they are shielded from jamming by the terrain.)

**(3) Techniques.** A method of accomplishing a goal or mission. (Example: Use quick (hasty) informal fire support planning as soon as possible when it is essential to attack.)

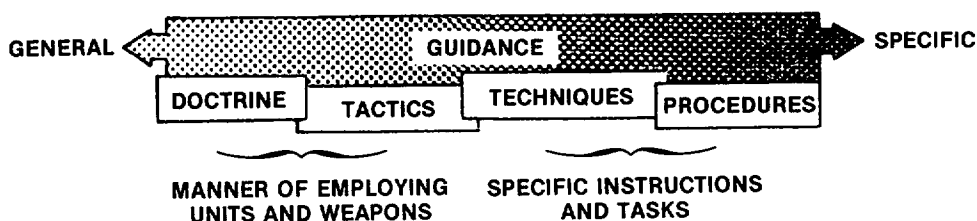


Figure 1-1. Relationship of Doctrine, Tactics, Tehniques, and Procedures.

**(4) Procedures.** A series of standardized steps. A particular way of doing something. (Example: Submit requests for jamming support on a Joint Tactical Electronic Warfare Request Form.) Obviously, there are no clear divisions between doctrine and tactics, tactics and techniques, and techniques and procedures. They inevitably blend together.

**b.** Employing units in combat is an art, (something acquired by experience, study, and observation), not a science, (something done by applying formulas). How a unit will be employed in combat depends on the mission, enemy, terrain and weather, and troops and fire support available. Doctrine and tactics help an individual master the art of employing units in combat, and they help a competent commander determine how to employ his unit. They are not substitutes for experience, study, and observation. Techniques and procedures, on the other hand, are specific ways, formulas to do things. For example, a specific format is used to request jamming support and the electronic warfare appendix is written in a specific format. This standardization makes the tasks they cover easier to do. The electronic warfare officer who uses the standard format for requesting jamming support provides all the information the electronic warfare agencies will need to provide the requested support, and the commander who uses the operations order format presents his guidance on electronic warfare in a form easily understood by others. The following example contrasts doctrine and tactics from techniques and procedures. Doctrine and tactics guide commanders when considering how to conduct electronic warfare activities. Once the decision is made on what types of electronic warfare activities will be conducted, those who will

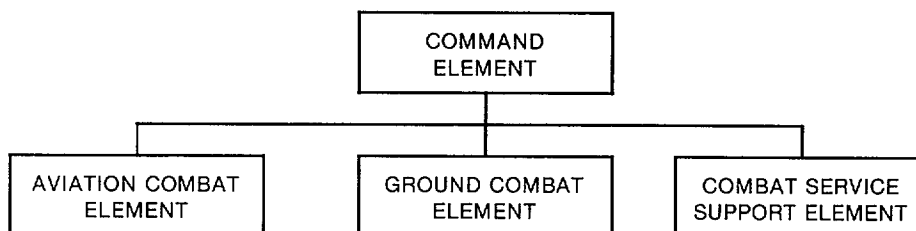
conduct the electronic warfare activities use the appropriate techniques and procedures.

## 1002. Structure of MAGTFs

Marine forces are employed in combat as Marine Air-Ground Task Forces (MAGTFs). A MAGTF has four elements: the command elements (CE), ground combat element (GCE), aviation combat element (ACE), and combat service support element (CSSE). (See fig. 1-2.)

**a.** The command element is the MAGTF headquarters. It is composed of the commander, the general or executive and special staff sections, the headquarters section, and the requisite communications and a limited service support capability. The establishment of a *single* headquarters over the aviation, ground, and combat service support elements provides the command, control, and coordination capability essential for effective planning and execution of operations. The establishment of this separate air-ground headquarters permits subordinate commanders to direct their attention primarily to the command of their respective elements. The MAGTF staff extends and complements the capabilities of the headquarters of major elements of the MAGTF, but should not duplicate them under normal circumstances.

**b.** The GCE is task-organized to conduct ground maneuver. It is constructed around an infantry or armored unit and varies in size from a reinforced battalion to a reinforced Marine division or divisions. The GCE also includes appropriate combat support units.



**Figure 1-2. Marine Air-Ground Task Force.**

c. The ACE of a MAGTF is task-organized to provide the required functions of Marine aviation. These functions—air reconnaissance, antiair warfare, assault support, offensive air support, electronic warfare, and control of aircraft and missiles—are provided in varying degrees based on the tactical situation and the size of the MAGTF. The ACE varies in size from a composite squadron to a reinforced Marine aircraft wing(s).

d. The CSSE is task-organized to provide combat service support to the MAGTF beyond the organic capabilities of the ACE, the GCE, and the command element.

### 1003. Training

Regardless of how well doctrinal and procedural publications are written, different people will interpret them differently. Further, the guidance in such publications can never be complete. Only by training in electronic warfare can the different interpretations be identified and reconciled. And only by training can the readers learn those subtleties which are commonly intended under the headings of judgment and experience.

### 1004. Standing Operating Procedures

Standing operating procedures (SOPs) should contain the information members of the units need to perform routine operations. SOPs should complement and not duplicate the publications of higher headquarters. Copies of these directives from higher headquarters should be made available to the individuals who need the information these directives contain.

### 1005. Signals Intelligence

Signals intelligence is a category of intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. Also called

**SIGINT.** (Joint Pub 1-02.) An understanding of signals intelligence is needed to understand electronic warfare. Components of SIGINT are—

a. **Communications Intelligence.** Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called **COMINT.** (Joint Pub 1-02.)

b. **Electronics Intelligence.** Technical and intelligence information derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called **ELINT.** (Joint Pub 1-02.)

c. **Telemetry Intelligence.** Technical information and intelligence information derived from the intercept, processing, and analysis of foreign telemetry. Also called **TELINT.** (Joint Pub 1.) (Telemetry intelligence is primarily strategic in nature and, therefore, is not addressed in this manual.)

d. **Foreign Instrumentation Signals Intelligence.** Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients. Foreign instrumentation signals intelligence is a category of signals intelligence. Note: Foreign instrumentation signals include but are not limited to signals from telemetry, beaconry, electronic interrogators, tracking/fusing/armoring/firing command systems and video data links. (Joint Pub 1-02)

### 1006. Signal Security

Signal security (SIGSEC) is a generic term that includes both communications security and electronics security. (Joint Pub 1-02.) SIGSEC is the state which results from actions; electronic counter-countermeasures are actions which contribute to that state. An understanding of SIGSEC is needed to understand electronic warfare. Components are—

**a. Communications Security.** The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC**. Communications security includes **a.** cryptosecurity; **b.** transmission security; **c.** emission security; and **d.** physical security of communications security materials and information.

1. **cryptosecurity** – The component of communications security which results from the provision of technically sound crypto-systems and their proper use.
2. **transmission security** – The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

3. **emission security** – The component of communications security which results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

4. **physical security** – The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

**b. Electronics Security.** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non-communications electromagnetic radiations; e.g., radar. (Joint Pub 1-02.)

# Chapter 2

## Electronic Warfare Doctrine

### 2001. General

Military forces depend on electronic equipment and the electromagnetic spectrum for communications, and for detection and identification of enemy forces. The use of the electromagnetic spectrum is, therefore, part of operations and intelligence. The force that selectively deprives the enemy of the use of the electromagnetic spectrum, or exploits its use by the enemy to obtain information, has an important advantage.

The actions taken to retain effective use of the electromagnetic spectrum by friendly forces and to exploit and degrade the enemy's use of this spectrum are collectively called electronic warfare.

**a. Electronic Warfare.** Military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of electromagnetic spectrum. Also called **EW**. There are three divisions within electronic warfare:

**a. electronic countermeasures** — That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Also called **ECM**. Electronic countermeasures include:

(1) **electronic jamming** — The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment, or systems.

(2) **electronic deception** — The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a

manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. Among the types of electronic deception are: **(a) manipulative electronic deception** — Actions to eliminate revealing, or convey misleading, telltale indicators than may be used by hostile forces. **(b) simulative electronic deception** — Actions to represent friendly notional or actual capabilities to mislead hostile forces. **(c) imitative electronic deception** — The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.

**b. electronic counter-countermeasures** — That division of electronic warfare involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of electronic warfare. Also called **ECCM**.

**c. electronic warfare support measures** — That division of electronic warfare involving actions taken under direct control of an operational commander to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support measures (ESM) provide a source of information required for immediate decisions involving electronic countermeasures (ECM), electronic counter-countermeasures (ECCM), avoidance, targeting, and other tactical employment of forces. Electronic warfare support measures data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT) and electronics intelligence (ELINT). (Joint Pub 1-02)

**b. Purpose of Electronic Warfare**

- To provide timely information on the enemy.
- To increase combat power by disrupting the enemy's use of the electromagnetic spectrum at critical times.
- To provide continued use of the electromagnetic spectrum despite enemy EW.

**c. Integration Into Operation.** EW operations must effectively support combat operations. To achieve this, the EW plan must be developed early, it must be fully integrated into the overall operational plan, and it must be continually updated in light of changes in the tactical situation. The need for updating is stressed: If the EW plan is not adjusted as the situation changes, ESM may not provide the needed types of information, and electronic countermeasures may have an adverse effect on friendly command, control, and communications.

**d. Coordination.** EW, to be effective, must be coordinated at all levels and among Services and allies. Procedures must, therefore, be established and practiced to effect a coordinated EW effort between supporting elements and units employing EW resources.

**e. Responsibilities**

(1) ESM and ECM (in the areas of mission support and threat warning) are executed by EW units only in response to taskings by supported commanders or higher headquarters. For self-production missions, units do not depend on higher HQ for employment authorization.

(2) Electronic counter-countermeasures are the responsibility of all users of electronic equipment.

**2002. Electronic Warfare Support Measures**

ESM systems provide immediate threat recognition and a source of information for immediate decisions involving ECM, ECCM, avoidance, targeting, and other tactical employment of forces. Specific examples of ESM capabilities include radar warning equipment installed on tactical aircraft for self-defense, the receiver suite of the tactical jamming system on board electronic warfare aircraft, and equipment used to determine the surface threat by a submarine. Examples of tactical use of ESM information include the physical maneuvering of an aircraft by a pilot to avoid a surface-to-air missile, jammer assignment by an ECM officer in response to a displayed signal, or decision by a commander not to surface a submarine due to a detected surface threat.

**a. Intelligence Support to ESM.** Accurate electronic order of battle information must be available in order to accurately program ESM equipment, such as radar warning and tactical jamming systems.

**b. ESM Support to Intelligence.** Detection information derived from ESM equipment can be rapidly disseminated as combat information should significant threats be encountered. Processing and analysis of recorded ESM information requires a varying yet generally longer time before dissemination is possible. At this point, ESM generally enters the arena of intelligence.

**c. Terms Related to ESM.** The following terms are often used in discussions of ESM.

(1) **Intelligence.** The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (Joint Pub 1-02) As an example, the emitter information displayed in the EA-6B

ceases to be ESM when it is recorded, processed, and reported by the ground processing system.

**(2) Information.** In intelligence usage, unevaluated material of every description that may be used in the production of intelligence. (Joint Pub 1-02) (Part one of two-part definition.)

**(3) Combat Intelligence.** That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Joint Pub 1-02)

**(4) Combat Information.** Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (Joint Pub 1-02)

**(5) Intelligence Requirements.** Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (Joint Pub 1-02) Intelligence requirements are stated in one of three forms:

**(a) Basic Requirements.** Items of information regarding the enemy and his environment. These state the requirements for basic intelligence.

**(b) Essential Elements of Information (EEI).** The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. (Joint Pub 1-02)

**(c) Other Intelligence Requirements (OIR).** Items of information desired regarding the enemy and his environment.

**(6) Collection Agency.** Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (Joint Pub 1-02)

**(7) Source.** A person, thing, or activity from which intelligence information is obtained. (Joint Pub 1-02) (Part one of three-part definition.)

## 2003. Electronic Countermeasures

**a. Electronic Jamming.** (Hereafter, jamming and electronic jamming are synonymous.)

**(1) Effect.** Jamming affects receivers, not transmitters. It overrides the signals the receiving station hoped to receive with more powerful signals transmitted by the jamming station.

**(2) Control.** Because of its possible impact on friendly communications and noncommunications emitters (e.g., radars and data links), jamming will normally require centralized control (authority). However, in certain situations, control (authority) may be delegated to lower commanders.

**(3) Modes.** There are many types of jamming modulations. The type used in a given situation depends on the ECM equipment available, the characteristics of the victim emitter, and the desired effect. There are two categories of jamming: active jamming and passive jamming.

**(a) Active Jamming.** Active jamming is jamming that uses original signals. Common types of active jamming are spot, barrage, and sweep jamming.

**1** In spot jamming, the power is concentrated on one channel or frequency.

2 In barrage jamming, the power is spread over several frequencies or channels simultaneously.

3 In sweep jamming, the power is concentrated on one or a few frequencies at a time but is swept or moved over a large range of frequencies.

**(b) Passive Jamming.** Passive jamming is jamming that repeats signals. It includes jamming executed with repeaters, transponders, chaff, and reflectors.

1 Repeaters intercept a signal, alter it, amplify the altered version, and retransmit it.

2 Transponders automatically transmit a predetermined signal when the transponder receives a predetermined signal.

3 Chaff is narrow metal strips or coated paper of various lengths and frequency responses. It is used to reradiate radar signals. These reradiated signals produce false targets.

4 Reflectors, such as corner reflectors, consist of flat reflecting surfaces connected to form three-dimensional reflectors. They are used as decoy radar targets.

**(4) Concentration.** Indiscriminate employment of jamming must be avoided. The best results are obtained when resources are concentrated to simultaneously disrupt or degrade all types of electromagnetic communications and/or noncommunications systems (e.g., radar and data links) of selected enemy units, formations, or weapons systems that have a direct impact on the accomplishment of our mission.

**(5) Timing.** Jamming is effective for a limited time only because the enemy will use counter-countermeasures to overcome jamming effects. To be effective, jamming must be brought to

bear quickly at the critical time and place. Maximum effectiveness will be obtained if the attack is delivered at a critical time against a critical enemy electronic system (e.g., fire control nets during his attack, air defense systems during friendly offensive air operations, command and control communications for the control of the movement or commitment of reserves).

## **(6) Planning and Employment**

**(a)** To jam, the frequencies being used by the target stations must be known and a favorable *jamming-to-signal ratio* (JSR) must be achieved over the receiving station. A favorable JSR means the jamming signal received at the target-receive antenna is stronger than the enemy signal intended for that same target-receive antenna. This ratio is influenced by the location and effective radiating power of the jammer, the terrain and distance between the jammer and the station being jammed, and the characteristics of the jammers antenna and the target's antenna (e.g., beamwidth, polarization, degree of side/back-lobe suppression).

**(b)** Jamming must be recognized as a complementary option to attack the enemy where other methods, such as fire support, are not more suitable or are not available. Jamming operations must be integrated into overall attack planning. Jamming is a means to an end, not an end in itself. Some of the activities jamming can support are—

1 Hindering command and control by impeding or disrupting communications and data links between elements of a force; denying or delaying radar early warning, ground control intercepts and target acquisition and tracking; and defeating or degrading critical links inherent in surface-to-surface and surface-to-air weapons systems (missile beacons or seekers).

**2** Intelligence collection by prompting a unit to transmit in the clear rather than over secure communications circuits.

**3** Causing communication or noncommunication equipment shortages by making it appear that radio, data link, teletype, and radar equipments are not operating properly.

(c) Jamming may be preplanned or in response to an immediate tactical situation.

(d) In deciding upon electronic jamming, commanders and staffs must carefully weigh the operational requirement against the restrictions or effects imposed on friendly systems and the loss of information about the enemy otherwise obtained by electronic warfare support measures. Degradation of some friendly command and control communications may have to be accepted in order to effectively employ jamming. Jamming's greatest weakness is that it may indicate to the enemy what we know about the frequencies he is using. And knowing this, he may change his frequencies, if capable, making further jamming difficult and making ESM much less productive.

(e) Jamming can be done with varying degrees of subtlety. It may be obvious or subtle. Although the examples contained in the following subparagraphs specifically relate to communications jamming, analogous discussions can be made concerning the jamming of noncommunications receivers (e.g., radars and data links).

**1 Obvious.** Jamming so conducted that the enemy can easily detect it. Often noises are used to simultaneously attack most of a unit's communications nets. Some obvious jamming signals are—

**a Random Noise.** This is synthetic radio noise. It is random in amplitude and frequency. It is similar to normal background noise and can be

used to degrade all types of signals. Operators often mistake it for receiver or atmospheric noise and fail to take appropriate ECCM actions.

**b Stepped Tones.** These are tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are normally used against single-channel AM or FM voice circuits.

**c Spark.** The spark signal is easily produced and is one of the most effective for jamming. Bursts are of short duration and high intensity. They are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications.

**d Gulls.** The gull signal is generated by a quick rise and slow fall of a variable radio frequency and is similar to the cry of a sea gull. It produces a nuisance effect and is very effective against voice radio communications.

**e Random Pulse.** In this type of interference, pulses of varying amplitude, duration, and rate are generated and transmitted. They are used to disrupt teletypewriter, radar, and all types of data transmission systems.

**f Wobbler.** The wobbler signal is a single frequency which is modulated by a low and slowly varying tone. The result is a howling sound which causes a nuisance effect on voice radio communications.

**g Recorded Sounds.** Any audible sound, especially of a variable nature, can be used to distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.

**h Preamble Jamming.** This type of jamming occurs when the synchronization tone of speech security equipment is broadcast over the operating frequency of secure radio sets. Preamble jamming results in all radios being locked in the receive mode. It is especially effective when employed against radio nets using speech security devices.

**2 Subtle.** This type of jamming is not obvious. The aim of subtle jamming is to leave the operator unaware he is being jammed. He does not receive an incoming friendly signal and everything appears normal.

**a** With equipment which must be synchronized, subtle jamming may be used to break the synchronization, thus giving the appearance that the equipment is broken.

**b** It should be noted that the radio operator should determine if his radio is being jammed in all other function control modes. These other modes must be checked. Far too often, we make the mistake of assuming that our radios are malfunctioning instead of recognizing the subtle jamming for what it is.

**(f) Jamming,** like all warfare techniques, is most effective when used against an enemy who is not prepared for it. Jamming for the purpose of harassing the enemy or gaining or supporting a minor operation is usually counterproductive because it assists the enemy in determining his vulnerability to jamming and because it helps his operators learn to recognize our jamming and to work through it. Indeed, jamming is usually effective for a limited time only. The enemy usually will take whatever measures are necessary to overcome the effects of jamming.

## (7) Minimizing Interference

**(a)** Electromagnetic interference is any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. Also called **EMI**. (Joint Pub 1-02)

Often communication and noncommunication electronic equipment is disrupted not by enemy jamming, but by unintentional EMI from friendly sources. Therefore, it is important that users and operators of electronic equipment be familiar with, understand, and be able to recognize and minimize the effects of EMI caused by friendly electronic equipment. FMFM 3-3F, *Guide to Electromagnetic Interference Control*, discusses how to minimize EMI from friendly equipment.

**(b)** Frequencies which, for various reasons, should not be jammed are classified and listed as follows:

**1 TABOO Frequencies.** Frequencies of such importance that they must never be jammed. They may be critical to friendly force activities (e.g., command and control) or in use by the enemy and of exceptional importance for intelligence gathering.

**2 Guarded Frequencies.** Frequencies in use by the enemy and of use as a source of intelligence to the friendly force. Jamming activities on these frequencies are normally controlled by intelligence staffs.

**3 Protected Frequencies.** Frequencies allocated for operational use by the friendly force and on which jamming must be minimized.

(c) To reduce interference, friendly units should be advised of preplanned and, when feasible, immediate ECM activities.

(d) Interference that results from enemy ECM, is eliminated or minimized by planners and operators using appropriate ECCM techniques. See paragraph 2004 for a detailed discussion of ECCM.

## **b. Electronic Deception**

### **(1) General**

(a) Electronic deception is the use of electromagnetic energy in a manner intended to mislead the enemy in the interpretation or use of information received by his electronic systems. The three categories of electronic deception are defined in appendix D.

(b) Electronic deception is one of four types of deception. The other three types are: sonic, visual, and olfactory. Electronic deception is employed to cause the enemy to misinterpret what is received by electronic systems. Normally, it is conducted as part of a larger deception operation. To be most effective, deception operations should complement the actual concept of operations and must be well protected by operations security measures.

(2) **Application.** Electronic deception on a large scale is expensive in preparation time and resources. For electronic deception to be effective, it must be complemented by sonic, visual, and olfactory deception. The advance in electronic sensor technology and the speed with which information can be transmitted, received, correlated, and displayed for evaluation and decision making makes it extremely difficult to execute a large electronic deception effort with any degree of success. The enemy is likely to discover large deception efforts unless they are planned in detail and supported generously with personnel and equipment. Deception efforts are more likely to succeed if designed to achieve a specific objective that is

limited in time and scope. Land forces are, therefore, more likely to make use of limited scale deception operations at selected key times in the battle. Electronic deception should be conducted as part of an overall deception plan.

(a) **Coordination and Control.** Deception operations, like jamming, normally require centralized coordination and control.

(b) **Planning and Employment.** The employment of electronic deception, like jamming, must be integral to staff planning and must support the overall operation plan. Missions are normally preplanned but may be immediate if opportunities for limited application become available.

(c) **Imitative Electronic Deception (IED).** IED which involves the transmission of false voice commands to enemy units requires personnel who are exceptionally fluent in the enemy's language; i.e., can use enemy dialects, slang, and terminology. The availability of such personnel must not be taken for granted. IED varies in scope based on the sensitivity of the intelligence and the sophistication of techniques and equipment used. It could include nuisance intrusion, planned message intrusion, cryptographic intrusion, or deception intrusion. All but nuisance intrusion require extensive technical support and specially skilled operators. Nuisance intrusion requires only compatible radio equipment and foreign language ability. All require specific authorization from the senior headquarters controlling the operation.

## **2004. Electronic Counter-Countermeasures**

Generally, the measures included under the heading of ECCM are also included under the heading of good communications procedures. If communications are properly planned and executed, most of the measures needed to minimize the vulnerability of friendly units to enemy ECM and ESM will be

accomplished. Similarly, if the use of noncommunications electronic equipment (such as radar and data links) is properly planned and executed, most of the measures needed to minimize the vulnerability of units that depend on such equipment will be accomplished.

**a. Technical Protection.** The technical aspects of ECCM must be considered when equipment acquisition programs are initiated. Additionally, these programs must be reviewed when ECM vulnerabilities are detected.

**b. In Combat.** ECCM are practiced through the application of good training, sound procedures, and for countering communications jamming. All operators, users, and planners of electronic equipment must thoroughly understand the threat to and the vulnerability of their equipment to enemy ECM efforts and ensure that they take appropriate actions when attacked.

**c. Updating.** Procedural or operational measures must be continually adjusted to the tactical situation and must be included in all stages of staff planning and collective/individual training. ECCM can provide information on enemy ECM actions that will assist in developing the procedural or operational adjustments required to update ECCM procedures.

**d. Classification of ECCM.** There are two classes of ECCM: preventive and remedial.

**(1) Preventive ECCM.** These are the measures taken by commanders and staff officers when planning. It includes the selection of a scheme of maneuver which will minimize friendly electronic emissions that the enemy can intercept or disrupt using his ESM and ECM capabilities. This can be done by, among other ways, having a simple scheme of maneuver which can be executed with few or no emissions, by imposing radio silence, or by selecting avenues of approach which will interpose terrain

between friendly transmitters and enemy intercept stations. Preventive ECCM also includes measures to minimize the vulnerability of friendly receivers to enemy jamming.

**(2) Remedial ECCM.** Remedial measures are those taken by operators when the enemy jams our transmissions. Specific procedures are discussed in chapter 6.

## 2005. Communications

The need for immediate passage (near real time) of ESM-obtained information and jamming support can only be adequately met if dedicated secure and automated communications systems are available to the EW system and its major users, and there exists a clearly defined, easily understood reporting procedure.

In order to decrease the vulnerability of these dedicated communications systems, they should not present a unique communications signature in comparison to other systems on the battlefield.

## 2006. Authority of Commanders and Their Staffs

**a. Responsibility.** The responsibility of the commanders for their commands is absolute except to the extent that the commander is relieved of responsibility by competent authority or by regulations. While the commander may delegate authority to subordinates for the execution of details, such authority does not relieve the commander of responsibility for the safety, well-being, and efficiency of the entire command. The commander shall ensure that the delegated authority is properly exercised and that orders and instructions are properly executed. (Marine Corps Manual)

**b. Authority.** The authority of the commander is equal with the commander's responsibility, subject to the limitations prescribed by law and regulations. (Marine Corps Manual)

**c. Delegation of Authority.** When not contrary to law or regulations, commanders may delegate specific authority to their subordinates to assist in the performance of their command functions. However, commanders retain full responsibility for the performance of those duties which are delegated. Commanders must ensure that delegated authority is properly exercised and that orders and instructions are properly executed. (Marine Corps Manual)

**d. Staffs.** Staffs exist to advise and assist their commanders and to support subordinate commanders. All staff officers provide information and advice, make estimates and recommendations, prepare plans and orders, advise other staffs and subordinate commands of the commander's plans and policies, and supervise the execution of plans and orders. Staff officers have no authority as staff officers over any unit; however, staff officers may be delegated authority by the commander.

## 2007. Control and Coordination

To understand the responsibilities of the agencies and headquarters involved in EW, one must understand the terms command, control, and coordination and how variations of these terms are used in discussion on the supporting arms.

**a. Command.** The authority that a commander in the military Service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. (Joint Pub 1-02) (Part one of three-part definition.)

**(1) Components of Command.** The components of command are—

**(a) Operational Control.** Transferable command authority which may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in Combatant Command (command authority) and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations; normally this authority is exercised through the Service component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called **OPCON**. (Joint Pub 1-02)

**(b) Administrative Control.** Direction or exercise of authority over subordinate or other organizations in respect to administrative matters such as personnel management, supply, services, and other matters not included in the operational missions of the subordinate or other organizations. (Joint Pub 1-02)

**(c) Coordination.** (See par. 2007c.)

**(d) Technical Direction.** The performance of a specialized or professional service, or the exercise of professional guidance or direction through the establishment of policies and procedures in technical matters. Technical direction may include—

- Establishing standards or procedures for performing a technical function.
- Providing professionally trained and qualified personnel to perform a technical function.
- Providing professional advice, guidance, or assistance.
- Performing a technical function as a service to the command. (Marine Corps Manual)

(2) The components of command cited are not all inclusive. There is more to command than is included within these components of command.

**b. Control.** Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (Joint Pub 1-02) (Part one of four-part definition.) This is a very general definition. For an expression using the term to be useful in military operations, the meaning of control in that particular circumstance must be stated. Specifically, the authority must be defined and the activities over which this authority can be exercised must be stated. Without such clarification, a statement using the word control is useless because of its vagueness.

**c. Coordination.** (1) The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as: emergency defense measures; area intelligence and security; area public and labor relations; common supply; utilities; public works; leases and space assignments; transportation; prescription of area uniform regulations; sanitation and health measures; area maintenance of standards in discipline, legal assistance, and welfare; and other situations in which coordination is considered necessary. (Marine Corps Manual) (2) The act of bringing things into a common action, movement, or condition in order to achieve a specific goal.

## 2008. Ground Electronic Warfare

The capabilities and characteristics of ground electronic warfare assets are markedly different from those of aviation electronic warfare assets. This and the next paragraph discuss these capabilities, characteristics, and requirements.

### a. Characteristics

(1) Generally used to support GCE, however, is used as MAGTF commander deems necessary.

(2) Generally, EW equipment is employed on highly mobile platform. Where possible, this equipment should have the same mobility and survivability as the supported force.

(3) In order to avoid losses in signal strength, antennas are often not remoted.

(4) Most jamming is spot jamming.

(5) Direction finding and ECM sites are usually located in the forward area of the battlefield, with or near forward units due to short-range nature of tactical signals.

(6) Primarily directed against communications systems vice noncommunications systems unless offensive in nature.

### b. Requirements

(1) Protection from enemy ground and air forces by the supported unit.

(2) Logistical support for ECM and ESM elements operating with forward elements.

(3) Clear identification of EW requirements of the supported commander.

### c. Capabilities

- (1) Is best suited to support operations of ground units.
- (2) Can be positioned and protected to allow it to continue operating during an enemy attack.
- (3) Responsive to EW requirements of supported ground commander.
- (4) Can support aviation units or the MAGTF in general support (i.e., jamming of enemy air defense, C<sup>3</sup> during an air attack, in coordination with VMAQ jamming of air defense radar).

### d. Limitations

- (1) Can be overrun by enemy.
- (2) Can be masked by terrain.
- (3) Distance/propagation characteristics of enemy electronic systems.
- (4) ECCM actions employed by the enemy.
- (5) Vulnerable to enemy electronic deception.

support is very critical in aviation operations. It is this necessity for timeliness that forces the development of an extensive data base and necessitates much more detailed planning than that required to successfully support ground operations.

### a. Characteristics

(1) Airborne-related ECM activities are normally conducted in direct support of other tactical aviation missions. Airborne ECM operations may directly support assigned mission aircraft, they may be part of planned deception operations, or they may be in support of other MAGTF operations. Airborne ECM and threat warning operations require just as detailed planning and integration of the EW activities with the supported activities as is required for EW operations by ground units.

(2) Airborne ESM activities are usually conducted in general support of the MAGTF. ESM mission results are normally disseminated by the VMAQ detachment directly to elements without and external to the MAGTF as directed by the MAGTF commander. Paragraph 3003 explains this process.

(3) Usually has same mobility as supported force.

(4) The Marine Corps has two platforms that are designed to perform ESM and ECM in support of strike missions: the EA-6A and EA-6B aircraft.

(5) Special platforms to perform ESM and/or ECM mission in support of MAGTF operations may be requested through JTF/theater commander.

(6) Most Marine Corps aircraft are equipped for combat with self-defense ESM and/or ECM capabilities.

(7) Generally vital to successful air operations against modern air defenses.

## 2009. Airborne Electronic Warfare

In principle, the procedures followed in planning and executing airborne electronic warfare are similar to those followed on the ground side. As noted earlier there are, of course, differences in specific capabilities and equipment characteristics, but the most significant difference between ground and airborne support requirements is in terms of time. Aviation engagements are generally much shorter and they are conducted at much higher speeds than ground engagements. Consequently, the timeliness of EW

(8) Primarily directed against noncommunications line-of-sight systems (radars) and is used for description of enemy air defense systems.

## **b. Requirements**

(1) Protection from enemy air defense. Aircraft conducting ESM and ECM usually must fly straight and level.

(2) Proper radial and elevation alignment between the jamming platform and the attack aircraft being supported. This is very important. For it to occur, there must be detailed liaison between the aircrews of the aircraft providing the EW support and the aircrews being supported.

(3) Large ground support facilities.

(4) Extremely sophisticated equipment to detect, identify, exploit, and engage enemy noncommunications systems.

(5) Highly trained collection and analytical personnel.

(6) Clear understanding of the EW needs of the supported commander.

## **c. Capabilities**

(1) Airborne ECM operations are best suited to support air operations.

(2) Airborne ESM or threat warning operations may support both the ACE and the MAGTF as a whole.

(3) Extended EW range over that offered by ground assets.

(4) Possess greater mobility and flexibility than possessed by ground assets.

(5) Can support MAGTF or ground forces in general support role (i.e., jamming of counterbattery radars, etc.).

## **d. Limitations**

(1) Number of the platforms in the Marine Corps. This means that a MAGTF will usually have very few EW aircraft.

(2) Time on station before fuel/crew considerations require platform to return to base.

(3) Vulnerable to enemy ECCM actions.

(4) Vulnerable to enemy electronic deception.

(5) Although the effective ranges at which ESM and ECM can be conducted by aircraft are greater than those of ground EW assets, line-of-sight limitations (i.e., terrain masking and radar horizon) still apply.

# **2010. Electronic Warfare in Various Types of Operations**

This paragraph discusses *some* of the ways electronic warfare can be conducted in various types of operations.

## **a. EW Support to Offensive Operations**

(1) The commander must ensure that the EW systems are so deployed that they can provide early information for all stages of his attack. The nature of offensive operations will demand that EW units are deployed well forward in order to develop the EW information base for further EW support to operations.

(2) In an attack against a well-established defensive position, the ground EW advantage will rest with the defender due to alternate communication means available to him. In the attack, EW should emphasize—

- Detection, location, and disruption of enemy surveillance and target acquisition systems, in particular air defense, counter-battery and countermortar radars.
- Detection and location of the reserve and counterattack elements.
- Electronic isolation of selected enemy units or formations by disruption of communications with their flank units, higher formations, and reserves.
- Location of enemy ECM elements so they may be eliminated by physical attack.

**b. EW Support to Defensive Operations.** EW in support of defensive operations will consist of the following:

(1) Primary tasking will be the continued development of an EW information base. An EW data base will contain an electronic order of battle, a compilation of enemy communications capabilities, enemy command and control structure, and technical data on enemy communications such as frequencies and call signs. ESM will be vital for acquiring information on the enemy's—

- Leading elements.
- Grouping, location and axis of advance of the main body, and forces in depth.
- Activity concerning nuclear delivery systems.
- Intentions (required for future analysis).

(2) As the enemy closes to the main defensive position, ECM should be concentrated on the disruption of enemy fire control and target acquisition systems. While ESM resources continue to provide information for ECM

operations, they will attempt to determine enemy concentrations, direction of movement, and timing of the assault.

(3) EW operations must support friendly command and control systems by attempting to accurately locate enemy ECM assets so they may be neutralized by means such as physical destruction.

**c. EW Support to Delaying Operations.** The delaying force should employ EW resources to disrupt and confuse the advancing enemy by use of ECM against reconnaissance elements, battalion and regimental command nets, and fire control nets. ECM resources may assist the delaying force in breaking contact.

**d. EW Support in the Advance to Contact.** In the advance, ESM operations will focus predominately on ascertaining the location, strengths, and if possible, the intentions of the enemy. If EW resources are provided to the covering force, ECM resources should be employed to isolate forward enemy elements.

**e. EW Support in the Withdrawal.** EW operations must assist to achieve breaking contact with the enemy. Jamming and deception should be employed to disrupt and deceive the enemy electronic warfare and surveillance systems as to intention, timing, and direction of withdrawal. ECM assets should assist in denying information on further operations to the enemy. ECM can provide an electronic screen for friendly command and control systems used to coordinate the withdrawal. ECM can be used to disrupt enemy command and control nets so as to slow enemy reactions to information they may have obtained concerning the friendly withdrawal.

# Chapter 3

## Electronic Warfare Resources

### 3001. General

To provide EW support to Fleet Marine Force units, the Marine Corps has two types of EW units: radio battalions and Marine tactical electronic warfare squadrons (VMAQs). Most Marine Corps units with staffs have special staff officers to advise the commander and the rest of the staff on EW.

### 3002. Radio Battalion

a. The battalion mission is to conduct ground-based EW. The 1990s will see a gradual expansion of radio battalions operating from rotary to fixed-wing assets.

b. 1st Radio Battalion is located at Kaneohe Bay, Hawaii, and 2d Radio Battalion is at Camp Lejeune, North Carolina.

c. The radio battalion assists in generating technical data on enemy communication/electronic order of battle (COB/EOB) for the G-2/S-2 to correlate with other intelligence in support of MAGTF operations.

d. The radio battalion may be tasked to conduct ECM against selected enemy communications or communications nets to disrupt enemy operations. Because ECM can also interfere with friendly communications and because ECM should support the accomplishment of the MAGTF commander's mission, ECM are coordinated with

other operations in the signals intelligence/electronic warfare coordination center (S/EWCC).

e. Radio battalion support is usually requested through the SRIG (surveillance, reconnaissance, and intelligence group) commander.

f. See FMFM 3-23, *Signals Intelligence/Electronic Warfare Operations* (C).

### 3003. Marine Tactical Electronic Warfare Squadron

a. VMAQ-2, 2d Marine Aircraft Wing, and VMAQ-4, 4th Marine Aircraft Wing, are the only specialized Marine airborne EW units. Their primary mission is to provide EW in support of Fleet Marine Force operations.

b. The VMAQs provide EW support primarily in the following areas:

(1) ECM support for strike force aircraft to prevent, delay, or interrupt detection and tracking by enemy early warning (GCI), acquisition, and fire/missile control radars. ECM operations may also be conducted against the elements within a surface-to-air weapons system (i.e., missile seekers, missile beacons, target tracking/acquisition radars) to prevent effective engagements or increase miss distances.

(2) ESM operations are conducted to develop and maintain EOB, to include both selected emitter parameters and emitter location of non-friendly emitters. Additionally, aircraft ESM capabilities may be employed to provide threat warnings for friendly aircraft, ground units, or ships (i.e., air-to-surface or surface-to-surface missile defense role).

(3) The VMAQs provide ECCM training to ships, aircraft, and ground units. By conducting routine ECM operations in peacetime against friendly radar systems, radar operators can receive training in how to work through jamming and how to employ their particular systems ECCM capabilities.

**c. Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES)**

(1) The AN/TSQ-90C TERPES is an integrated, land-mobile, air-transportable, data processing system organic to VMAQs. Each TERPES has three shelters with equipment and software capable of receiving, processing, evaluating, and reporting electronic reconnaissance information and tactical jamming data obtained from EA-6s. This information is recorded on a digital tape carried in the aircraft.

(2) TERPES-generated EOB reports contain information of use to the ground and aviation elements of a MAGTF and to forces external to the MAGTF. Normally, reports are generated and distributed in accordance with guidance provided by the MAGTF commander or in response to requests for specific information from the MAGTF commander or from some element of the MAGTF.

(3) TERPES is connected to the Marine Air-Ground Intelligence System (MAGIS) via the intelligence analysis center (IAC). (The IAC is the MAGTF commander's all-source integrated information processing center.)

Information is passed from TERPES to the IAC and other agencies in the form of the TERPES reports.

d. VMAQ aircrews use the tactical EA-6B mission planning system (TEAMS) to select the best flight tracks to identify emitters and threat systems in the vicinity of flight tracks, and create maps and logs for both their and the strike mission commander's use.

e. Although EA-6s can collect ESM data during ECM missions, the profiles and tactics used by EA-6s on ECM missions reduce the aircraft's ESM capabilities. Therefore, EA-6s should normally be tasked to provide ECM or ESM support on a given sortie.

f. See FMFM 5-10, *Air Reconnaissance*, and FMFM 3-23, *Signals Intelligence/Electronic Warfare Operations*, (C).

## 3004. Other Services

Marine forces normally operate in joint or combined operations. Forces from the other Services or nations will usually have EW assets. These assets can support MAGTFs or elements thereof. EW assets of other Services include the U.S. Air Force EF-111 and RC-135 aircraft, U.S. Army EW aircraft and CEWI battalions, U.S. Navy VAQ and VQ squadrons, U.S. Navy fleet EW support group and the Air Force EC-130H (Compass Call).

## 3005. National Level Agencies

Some aspects of EW are most efficiently done when handled by a single agency. The National Security Agency (NSA) and the Joint Electronic Warfare Center (JEWEC), Kelly Air Force Base, San Antonio, Texas, are two of these agencies.

**a. National Security Agency.** NSA provides several types of support to Marine units. The most notable of these are codes, cyphers, and encryption devices. The assets available to NSA enables them to produce and test code sheets and encryption devices more thoroughly than any Service and any local command. NSA also conducts operational ELINT and technical ELINT to support EOB maintenance and validation.

**b. Joint Electronic Warfare Center.** The JEWEC mission is to provide, upon request, technical assistance, comprehensive analytical support, and advice for the planning and execution of EW. The JEWEC supports the Secretary of Defense, the Joint Chiefs of Staff, the military Services, the unified and specified commands, and other Department of Defense (DOD) agencies. The JEWEC functions and responsibilities are to—

- (1) Serve as the DOD central point of contact for EW information. It provides direct inquiry service to DOD activities.
- (2) Provide combat and contingency EW planning support in the form of predictive analysis radar terrain masking overlays and targeting recommendations for DOD requests. It also evaluates EW effectiveness in combat.
- (3) Evaluate meaconing, intrusion, jamming, and interference (MIJI) incidents and issues hazard warnings, as required. It also identifies MIJI trends and maintains a national MIJI data base.
- (4) Act as the central point of contact for EW and command, control, and communication countermeasures (C<sup>3</sup>CM) lessons learned.
- (5) Upon request, provide a variety of services related to EW, such as—
  - Assist in the formulation, review, and evaluation of EW doctrine, policy, operational concepts, tactics, and techniques.
  - Assist in the formulation, review, and evaluation of C<sup>3</sup>CM doctrine, policy, operational concepts, tactics, and techniques.
  - Analyze the capabilities of U.S. EW systems in relation to existing and postulated systems.
  - Analyze EW vulnerabilities of command and control systems and electromagnetic-dependent systems and weapons, and recommend actions for improving the survivability of these systems in an EW environment.
  - Conduct studies on EW of an operational nature for DOD organizations.
  - Assist exercise planners during the preexercise, employment, and postexercise phases.

### 3006. Duties of Personnel

The personnel discussed in this paragraph are staff officers in the headquarters of the MAGTF and of division, aircraft wing, and force service support group (FSSG) units. As such, these officers have no inherent authority over the commanders of subordinate units. (See par. 2006.) The EW-related duties listed for each of these officers are generally those performed by them. These duties can be modified however the commander desires.

#### a. Intelligence Officer (G-2/S-2)

- (1) Directs the efforts for the collection of information derived by ESM.
- (2) Determines the intelligence required in conjunction with the G-3/S-3 for the planning and execution of ECM operations.
- (3) Plans, coordinates, and supervises ESM and signals intelligence operations.
- (4) Assists and advises in determining enemy targets for destruction or ECM.
- (5) Identifies enemy emitters which should be restricted targets because of their intelligence value.

### **b. Special Intelligence (SI) Officer**

(1) Oversees S/EWCC if he is senior to the EWO.

(2) Maintains close liaison with MAGTF intelligence operations center to ensure that the S/EWCC and SIGINT/EW sources attached to MAGTF have current combat information and intelligence.

(3) Supervises maintenance of S/EWCC maps.

(4) Supervises processing and sanitization of reports containing SI.

### **c. Operations Officer (G-3/S-3)**

(1) Plans, coordinates, and tasks EW operations and activities.

(2) Coordinates with the G-2/S-2 to establish priorities between EW and SIGINT missions.

(3) Coordinates with the communications-electronics officer (CEO) to facilitate maximum use of the electromagnetic spectrum through ECCM and minimize EMI.

(4) Plans for operations security (OPSEC), which includes SIGSEC.

(5) Plans deceptions.

**d. Electronic Warfare Officer.** The EWO performs the general duties of a general staff officer, under the staff cognizance of the G-3. With respect to EW, his staff duties include—

(1) Advising operations officer on EW.

(2) Assisting operations officer in integrating EW activities with the other activities of the command.

(3) Integrating the EW plan into both plans and orders and prepares EW appendixes to those orders and plans.

(4) If on the MAGTF staff, the EWO—

(a) Is OIC of the S/EWCC if he is senior to the SI officer.

(b) Maintains close liaison with MAGTF combat operations center (COC) to ensure that the S/EWCC and attached SIGINT/EW assets have current information on planned and ongoing operations.

(c) Prepares ECM taskings.

(d) Staffs ECM operations plans with G-2, G-3, CEO, and higher and adjacent headquarters.

(e) Supervises maintenance of ECM support file/ECM log.

(f) Supervises maintenance of joint tactical EW request file.

### **e. CEO/Communications Officer**

(1) Maintains a continuing COMSEC program in coordination with the EWO.

(2) Assists in the supervision of ECCM.

(3) Coordinates communication plan with EW plan.

(4) Advises commander on ECCM.

(5) Submits MIJI reports, as required.

## **3007. Signals Intelligence/Electronic Warfare Coordination Center**

S/EWCC is a Marine Corps staff agency where signals intelligence and electronic warfare operations are coordinated.

S/EWCCs are not standing organizations. They are formed when a headquarters needs one. Generally, only MEF and MEB headquarters have S/EWCCs. They provide an area where special intelligence material can be handled and stored. They are a forum to plan, monitor, and review EW activities. The S/EWCC is established and maintained by the G-2.

Some members of an S/EWCC have duties in addition to those they perform in the S/EWCC. While these duties may cause these members of the S/EWCC to be absent from the S/EWCC much of the time, these duties also expose these individuals to the information they need to be effective members of the S/EWCC.

Indeed for a member of an S/EWCC to be effective, he must know the needs and plans of his respective staff sections or unit.

In order to facilitate and expedite S/EWCC operations, it is important to ensure that an appropriate facility is provided for this organization. The specific area designated for the S/EWCC need not be extensive. It may simply be a corner of a tent. The important thing is to establish an area where those working on electronic warfare and signals intelligence can talk and maintain their records. Because of the nature of the material handled in the S/EWCCs, the area designated as the S/EWCC must be in a secure compound.

# Chapter 4

## Electronic Warfare Planning

### 4001. General

For electronic warfare elements to make the greatest contribution which they are capable of, planning of electronic warfare operations must be integrated with the planning of a force's other operations. Victory usually goes to the force which is the most effective overall. Electronic warfare is not an end unto itself.

As was indicated in paragraph 2001c, one of the keys to effective EW operations is the adjusting of plans as the situation changes. This requires those concerned with EW operations to keep abreast of the situation and to maintain and update their personal estimates of the situation. Whenever one receives information he must ask himself if this new information indicates a change in the situation, and if so, what is the situation now.

### 4002. ESM Plans

ESM, as should be clear from paragraph 2002, is part of the overall intelligence effort. Thus, the information acquired by ESM activities is disseminated through the same channels as intelligence, target data, and combat information. Indeed, information acquired through ESM activities is usually blended with other information or otherwise made to appear that it was acquired by other than ESM activities. Further, ESM support is usually not requested as such. Rather the usual system of EEI and OIR is used.

Exceptions to the above occur when EW collection assets can pass ESM and other information directly to a unit. Examples of this are the providing of a direct support team (DST) or direct support unit (DSU) from radio battalion to a headquarters or the

passing of TERPES-generated reports to various headquarters. In these cases, specific types of plans must be developed. See chapter 8 for details on developing plans for support and use of DST or DSU. VMAQ post mission reports are automatically generated and submitted to MAGTF and other units, as directed by the MAGTF commander. TERPES can also provide EW and intelligence reports in response to requests from other units in accordance with procedures established by the MAGTF commander. Since the TERPES automatically disseminates reports, recurring requirements for the information promulgated in TERPES reports should be requested as far in advance as possible. Paragraph 7003 contains additional information on TERPES reports.

### 4003. ECM Plans

#### a. Ground ECM Plans

(1) As was noted in paragraph 2003, ECM has limitations. These include the need for information on the structure of enemy radio nets and on the frequencies he is using (a technical data base). Another limitation is compromising the technical data base. The enemy may change the frequencies of the nets we jam. If the enemy uses the same frequencies for his important nets which we use for our important nets, ECM may be impossible. The provision of backup frequencies can overcome this problem.

(2) Usually, a commander requesting ECM support should describe only the operation to be supported and not attempt to list the frequencies and stations to be jammed. The object

of ECM operations is to disrupt the enemy's command and control while some important tactical evolution is occurring. ECM operations should reduce the enemy's combat power when we can best exploit this reduction. Communication systems are usually complex and provide several channels for passing requests for fires, requests for reinforcements, intelligence reports, and other critical messages. Thus, for example, an ECM plan which is intended to disrupt radio communications between an enemy unit and a supporting artillery unit must disrupt more than the nets used by enemy forward observers to request fire support.

**b. Requesting ECM Support.** ECM support is requested using the format prescribed by DD form 1976, Joint Tactical Electronic Warfare Request. (See app. B.) Only those lines needed are used. Figure 4-1 is a sample request for ECM support.

Line A:	001,
Line A1:	001
Line A2:	2
Line B:	DMA V795S
Line C:	2
Line D1:	Attack on enemy position by 3d Bn, 5th Mar
Line D2:	915 922 to 885 965 to 077 003
Line D3:	Cross line of departure at 0615, reach final objective 0645.
Line D4:	Battalion
Line G:	Disrupt enemy's command and control, particularly those which control supporting arms.

**Figure 4-1. Sample ECM Request  
by Ground Unit.**

**c. Developing ECM Plans.** Requests for ECM support are forwarded through the chain of command to the commander authorized to plan and conduct ECM operations. For operations involving assets of the radio battalions, this is usually the MAGTF commander. For airborne ECM support by EA-6s, this is usually the ACE commander. The commander authorized to

conduct ECM makes a tentative decision on whether or not to provide the requested support. This tentative decision is based on such things as the relative importance of the tactical activity being supported, competing requests, and the adequacy of the technical data base. If a tentative decision is made to provide the requested ECM support, the request is passed to the supporting EW unit.

Upon receiving the request for ECM support, the electronic warfare asset starts its planning. This planning is based on, among other things, intelligence the EW unit already has and on intelligence the EW unit receives from other elements of the MAGTF and from agencies external to the MAGTF.

**d. Staffing ECM Plan**

(1) ECM plans developed by EW units attached to the MAGTF headquarters or to one of its elements are submitted to the S/EWCC. The EWO staff these plans within the headquarters and with adjacent, supporting, and higher headquarters. The CEO reviews the plans to ensure that they will not disrupt command and control communications. The G-2 reviews the plans to ensure that they will not needlessly disrupt or stop collection of critical information and intelligence. Problems which arise during the staffing which cannot be resolved are referred to the commander or his designated representative, usually the G-3. Problems which arise during the staffing of the plan with adjacent, supporting, and higher headquarters must be referred to higher authority for reconciliation. Once all problems are identified and reconciled, the decision will be made whether or not to execute the plan, and if so, when. Usually the assistant chief of staff, G-3 makes the decision.

(2) ECM plans developed by adjacent, supported, and supporting headquarters should be coordinated by these headquarters with the MAGTF headquarters. The EWO will be responsible for staffing these plans with the

G-2, G-3, SRIG, and CEO. The headquarters which originated the plan will be advised of the problem and attempts will be made to resolve the problem. Problems which cannot be resolved will be referred to higher authority. The headquarters which originated the plan will also be advised when the staffing has been completed and no problems have been found.

(3) Figure 4-2 shows the sequence for staffing ECM plans developed by EW units directly under the MAGTF commander in the chain of command.

(4) Figure 4-3 shows the sequence for staffing ECM plans developed by units directly under a

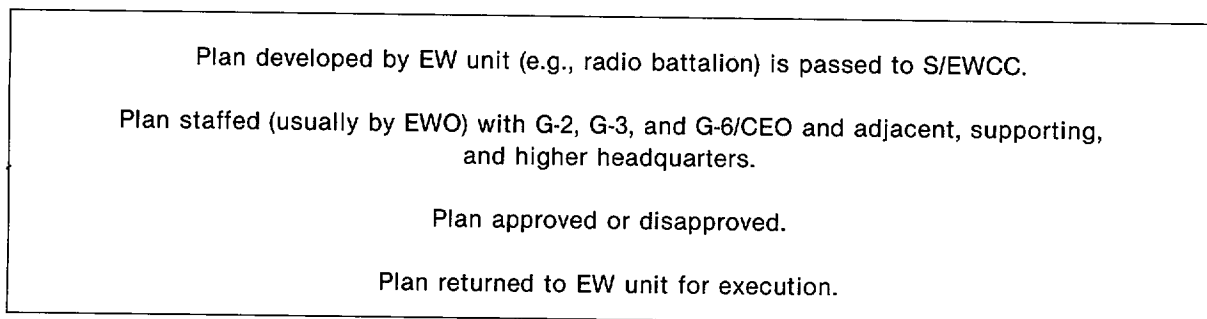
commander who is subordinate to the MAGTF commander in the chain of command.

(5) Figure 4-4 is a format that can be used by a commander to task EW units under him in the chain of command to conduct ECM operations.

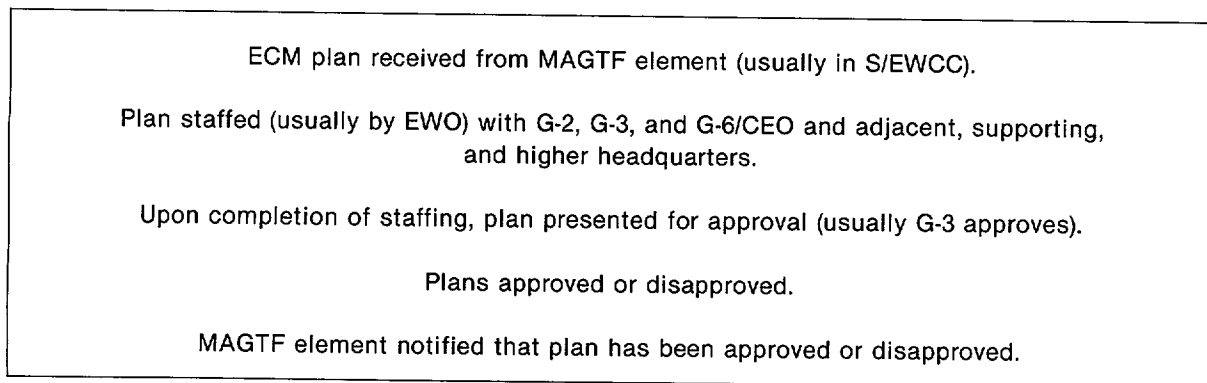
(6) Figure 4-5 is a sample ECM plan developed by an ECM unit.

(7) Figure 4-6 is a format for an ECM unit to use when reporting on ECM operations that element has conducted.

**NOTE:** Electronic counter-countermeasures are discussed in chapter 6.



**Figure 4-2. Staffing Sequence for ECM Plans Developed by EW Units Directly Under the MAGTF Commander in the Chain of Command.**



**Figure 4-3. Staffing Sequence for ECM Plan Developed by EW Unit (e.g., VMAQ-2) Directly Under a Commander Subordinate to the MAGTF Commander in the Chain of Command.**

1. Tasking of EW assets organic to the MAGTF headquarters will be prepared in the following format:

From: Commanding General

To: EW Asset

Subj: Tasking to plan ECM operations

1. Plan ECM operation to support following plan:

- a. Unit to be supported.
- b. Type of operation supported unit will be conducting.
- c. Coordinates of objective to be seized or defended by supported unit.
- d. Coordinates of supported units position at start of operation if different from that given in paragraph 3.
- e. Start time of operation. (Use local time.)
- f. Termination instructions. (Examples: Time, on request.)
- g. Amplifying data. (Example: Brief outline of scheme of maneuver.)
- h. Comments. Include any significant intelligence. (This information will be provided by G-2.)

2. Example:

From: Commanding General

To: DSU

Subj: Tasking to plan ECM operations

1. Plan ECM operation to support following plan:

- a. RLT-5
- b. Assault
- c. 721 214
- d. 702 211
- e. 0721

**Figure 4-4. ECM Planning Tasking.**

1. The following is an extract from a sample ECM plan developed by the DSU and approved by the Assistant Chief of Staff, G-3.

From: Commanding General  
To: DSU

Subj: ECM OPERATION PLAN 1-90

1. The following frequencies will be jammed by the following equipment:

62.50 1/04 BN TAC	AN/ULQ-19
61.50 1/84 BN TAC (ALT)	AN/ULQ-19
42.40 A/1/04	AN/ULQ-19
71-20 1/17 ARTY BN CMD	AN/ULQ-19

Approved. Execute at 100730U MAR 80.

J. L. STEELE  
By direction

**Figure 4-5. Sample ECM Plan.**

1. At the end of each ECM mission, the radio battalion DSU will complete and pass one of these to the S/EWCC on that mission. The report will be in the following format:

PRECEDENCE

DTG

FROM: DSU

TO: MAGTF HQ (Attn: S/WECC)

INFO:

CONFIDENTIAL (WHEN FILLED IN)

- A. Report number
- B. Type of ECM
- C. Period when jamming occurred
- D. Frequency jammed
- E. Location of jammer
- F. Unit jammed
- G. Type of jamming signal used
- H. Effect of ECM

**Figure 4-6. ECM Report.**

## Chapter 5

# Electronic Warfare Coordination and Control

### 5001. General

In electronic warfare, as with all aspects of military operations, there will be differences of opinion on how best to use assets. Such differences of opinion can be very strong. The consequences of decisions on such matters can be significant. Which answer is correct depends on the situation. In the military, differences of opinion are referred to the commander with the authority to resolve such conflicts.

As was noted in paragraph 2007b, control is “authority . . . exercised by a commander.” Thus, the commander who controls an EW unit or element has authority (control) over all or certain aspects of that unit’s or element’s activities. What or how much authority (control) depends on the type of control over the EW unit or element given to the commander.

### 5002. Command and Support Relationships

Command and support relationships are used to specify the authority of commanders over subordinate units and over supporting units. When establishing command and support relationships for EW units and elements, care must be taken to ensure that all parties concerned agree on the limits of the authority assigned by these relationships. Since the definitions of the command and support relationships are general, there is room for considerable disagreement on the limits of each of these forms of authority.

#### a. Definitions of Command Relationships

(1) **Command.** (See par. 2007a.)

(2) **Organic.** Assigned to and forming an essential part of a military organization. Organic parts of a unit are those listed in its table of organization for the Army, Air Force, and Marine Corps, and are assigned to the administrative organizations of the operating forces for the Navy. (Joint Pub 1-02)

(3) **Assign.** 1. To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function or greater portion of the functions, of the unit or personnel. 2. To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (Joint Pub 1-02)

(4) **Attach.** 1. To place units or personnel in an organization where such placement is relatively temporary. Subject to limitations imposed in the attachment order, the commander of the formation, unit, or organization receiving the attachment will exercise the same degree of command and control thereover as he does over the units and persons organic to his command. However, the responsibility for transfer and promotion of personnel will normally be retained by the parent formation, unit, or organization. 2. To detail individuals to specific functions where such functions are secondary or relatively temporary; e.g., attach for quarters and rations, attach for flying duty. (Joint Pub 1-02)

(5) **Operational Control (OPCON).** (See par. 2007a[2][a].)

(6) **Administrative Control (ADCON).** (See par. 2007a[2][b].)

## b. Definitions of Support Relationships

(1) **Direct Support.** A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance. (Joint Pub 1)

(2) **General Support.** That support which is given to the supported force as a whole and not to any particular subdivision thereof. (Joint Pub 1-02)

## c. Use of Command Relationships

(1) The command relationships are used to describe the authority of a commander over subordinate commanders. They are stated in a command's task organization. They apply to the operations of EW units and elements as much as to the operations of any other type of unit.

(2) During peacetime:

(a) 2d Radio Battalion is OPCON/ADCON to the 2d SRIG. 1st Radio Battalion is OPCON/ADCON to CG, FMFPac.

(b) VMAQ-2 is under the command of the Commanding General, 2d Marine Aircraft Wing, and VMAQ-4 is under the command of the Commanding General, 4th Marine Aircraft Wing.

(3) For exercises, deployments, or combat operations, the radio battalions, the VMAQs, or elements of these units may be placed under the control (authority) of commanders other than those listed above. If this is done, one of the command relationships will be used to specify the degree of control (authority). The relationship is stated in the appropriate task organization.

## d. Advantages/Disadvantages of Command Relationships for EW Units or Elements

(1) **Command.** This is vested in the Commanding Generals of Fleet Marine Forces, Atlantic and Pacific and cannot be delegated.

(2) **Organic.** Not applicable to this situation.

(3) **Assignment.** By its nature, assignment commits the EW unit or element to a commander on a relatively permanent basis. The principal advantage of this command relationship is that it facilitates long-range planning and training. However, since a unit or element can be assigned to only one commander at a time, this command relationship can limit flexibility and responsiveness from the perspective of the commanding generals of the Fleet Marine Forces; i.e., while assigned, the EW unit or element is only available to the commander to whom it has been assigned. For this reason, assignment is a very unlikely relationship.

(4) **Attachment.** Attachment has the advantage of cleanly placing a unit in an organization. Attachment is the most frequent command relationship between MAGTF commanders and EW units or elements during operations and exercises because (1) MAGTFs formed for operations or exercises usually have relatively temporary task organizations and (2) EW units or elements are placed in a task organization for the execution of specific operations plans or the conduct of a specific exercise. Attachment encompasses the authority included in OPCON and ADCON. For radio battalions and elements thereof, the disadvantage is that the expertise required to properly exercise this authority is usually found only on MEB and MEF staffs.

(5) **OPCON.** The comments on attachment also apply to OPCON except that the commander with OPCON does not have the authority included in ADCON. Since a unit's or element's effectiveness is very much dependent on having adequate supplies and proper

personnel, lack of this authority can limit the ability of the commander who has OPCON of an EW unit or element to conduct EW activities.

**(6) ADCON.** This form of authority is useful if, as with EW equipment and personnel, supplies of personnel and equipment are limited. A commander can ensure that EW units or elements over which he has ADCON receive the necessary personnel and supplies without depriving other such units or elements of needed personnel or supplies. The disadvantage of ADCON is that a commander with this authority may not be abreast of the tactical situation, and thus may not allocate personnel and equipment in a manner which best supports success in combat.

#### e. Support Relationships

**(1)** These relationships (direct and general support) are used when it is desired to have an EW unit or element support a commander while giving the supported commander very limited authority over the supporting EW unit or element. The distinctions between direct support and general support are vague. Usually the distinction is in the level of the headquarters being supported. For an EW unit or element, the term general support is usually used when the unit or element is supporting a MAGTF, and direct support is used if the EW unit is supporting only part of the MAGTF; e.g., the ground combat element of a MEF or an infantry battalion.

**(2)** These relationships are ideal when the supported unit does not have the expertise required to intelligently exercise the authority inherent in a command relationship. These relationships, therefore, are the ones most likely to exist between combat units and elements of radio battalions.

### 5003. Authority of Area Commander

When a commander is assigned an area (e.g., an infantry battalion commander who is assigned a

sector), he is given the authority (control) necessary to coordinate the actions of the separate organizations in his area on such matters as emergency defense and traffic control. The exercise of this authority is called coordination.

**a. Definition of Coordination.** 1. The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as: emergency defense measures; area intelligence and security; area public and labor relations; common supply; utilities; public works; leases and space assignments; transportation; prescription of area uniform regulations; sanitation and health measures; area maintenance of standards in discipline, legal assistance, and welfare; and other situations in which coordination is considered necessary (Marine Corps Manual). (Note: Coordination has two definitions. See paragraph 5005 for discussion of the other.)

**b. Exemption From Control of Area Commander.** The missions or tasks assigned to a functional commander may require that certain installations and activities of that commander be partially or wholly exempt from the command authority of an area commander in whose area they are located or within which they operate. Such exemptions will be specified by the authority who establishes the functional command. A radio battalion or a detachment thereof assigned, attached, or OPCON to a MAGTF will frequently be an exempted command. That is, elements of the radio battalion (or detachment thereof) that are located in the sectors and zones of action of infantry units to perform ESM and ECM functions may be exempted from the control of the infantry commanders. If this is to be the case, the MAGTF commander must specify such.

**c. Area Commanders' Responsibilities for Exempted Activities.** Area commanders may be assigned specific responsibilities with respect to exempted installations or activities, such as ECM or ESM elements. This is particularly true if enemy forces should traverse the area commander's area

of responsibility to attack the exempted installation or activity. For example, the commander of a Marine infantry regiment may be assigned the responsibility of providing security for ECM and ESM teams from radio battalion operating in his, the regimental commander's, sector.

## 5004. Tasking Authority

Tasking authority is the authority to direct an EW unit or element to conduct SI, ESM, or ECM activities. This form of authority or control is peculiar to electronic warfare.

## 5005. Coordination of EW

Coordination is the act of bringing things into a common action, movement, or condition in order to achieve a specific goal. (Note: This is one of two definitions of coordination. [See par. 2007c.] )

**a.** All of the activities of a force should be coordinated; i.e., brought into common action and directed towards the accomplishment of the mission. In EW, this means primarily that ESM and ECM be done so as to best contribute to the accomplishment of the mission and so as to minimize interference with the activities of friendly units.

**b.** Coordination is achieved either by (1) commanders adjusting their plans voluntarily so as to bring the actions of their commands into common action or (2) commanders being directed by a senior commander to take those actions necessary to bring them into common action.

**c.** S/EWCCs are established to provide a location where those actions necessary for the coordination of EW may be conducted. The members of an S/EWCC do not have any inherent authority over commanders. However, the commander served by the S/EWCC may delegate the necessary authority to personnel in the S/EWCC to direct subordinate commanders.

## 5006. Tasking of MAGTF Assets

Signals intelligence/electronic warfare (SIGINT/EW) assets directly under the MAGTF commander in the chain of command (usually only the radio battalion or a direct support unit from a radio battalion) will usually receive their taskings from the supported unit commander. These taskings can direct collection efforts or ECM activities. The taskings must be approved by the commander or his designated representative. Authority is delegated to individuals, not to agencies. For collection taskings, the assistant chief of staff, G-2, is usually delegated the authority to task SIGINT/EW assets. In addition, for ECM taskings, the assistant chief of staff, G-3, is usually delegated the authority to task SIGINT/EW assets.

SIGINT/EW assets in the task organization of elements of a MEB or MEF (usually only the Det, VMAQ-2/4, which is attached to the ACE) will be tasked through the commander of that element of the MAGTF.

**a. Collection Taskings.** These take three forms: EEI, OIR, and specific taskings and guidance on reports generated by the TERPES

**(1) EEI and OIR.** These provide guidance to all collection assets under the cognizance of the MAGTF headquarters.

**(2) Specific Taskings.** An example of one is: locate the enemy's command post. These taskings focus the efforts of the SIGINT/EW assets on areas of special concern of the G-2.

**(3) TERPES-Generated Reports.** TERPES is organic to VMAQ-2 and is deployed with the ACE to process the electronic information collected by EA-6Bs. The TERPES generates reports as explained in paragraph 7003. Specific guidance on the distribution of these reports and on the emitters to be reported on will be provided to the ACE in a tasking message which is written by the S/EWCC.

**b. Electronic Countermeasures Tasking.** There are two types of ECM taskings: those to plan ECM operations and those to execute ECM operations.

**(1) Tasking to Plan.** As soon as it is determined that an ECM plan should be developed, the EWO will draft a tasking to develop an ECM plan. This tasking will usually be signed by the assistant chief of staff, G-3. It will include information on the operation the ECM plan will be supporting. Figure 4-4 contains a sample tasking to develop an ECM plan. The detailed planning of ECM operations is done by the EW units which will, if the plan is approved, execute it.

**(2) ECM Execution Tasking.** Once an ECM plan is developed in response to a tasking, it will be passed to the EW unit by the EWO with the appropriate annotation. Figure 4-5 is a sample of an approved ECM plan. Chapter 4 provides guidance on the staffing of ECM plans.

**c. Approving ECM Plans Developed by Subordinate Elements.** The ECM plans developed

by the EW units attached to a subordinate element of the MAGTF will be approved by the MAGTF commander or his designated representative, usually the assistant chief of staff, G-3. Upon receiving an ECM plan from an element of the MAGTF, the S/EWCC will staff the plan with the CEO, G-2, and adjacent, supporting, and higher headquarters. Once staffed, the S/EWCC will submit the plan to the assistant chief of staff, G-3, for his approval and then return the approved plan to the subordinate element.

**d. Tasking by Higher Authority.** Collection or ECM tasking from higher authority will be delivered to attached SIGINT/EW units through the MAGTF headquarters.

## **5007. Requests for External Signals Intelligence, EW, and SI Support**

Requests for SIGINT, EW, and SI support from higher and adjacent headquarters will be prepared by and submitted through the MAGTF.

## Chapter 6

# Electronic Counter-Countermeasures Techniques

### 6001. General

a. ECCM is that division of electronic warfare involving actions taken to retain effective friendly use of the electromagnetic spectrum.

b. FM 24-33, *Communications Techniques: Electronic Counter-Countermeasures*, provides basic guidance on communications aspects of ECCM. This chapter supplements the guidance contained in FM 24-33. Both FM 24-33 and this chapter are written for those who are not communications specialists.

c. ECCM is the one branch of EW which is practiced by all units.

d. ECCM is divided into two parts:

(1) **Preventive ECCM.** Those electronic counter-countermeasures taken during training, planning, and the establishment of communications and noncommunications-electronics systems.

(2) **Remedial ECCM.** ECCM taken when confronted with enemy use of EW.

to reestablish communications by laying wires, setting up new antennas, moving antennas, or using other remedial measures when the enemy jams all or most of the radio nets a battalion uses to communicate with higher and supporting headquarters. If the enemy is attacking in conjunction with his jamming, remedial measures may be totally inadequate for reestablishing communications. And once the enemy has ascertained our dispositions and intentions because we did not take the necessary preventive measures, no remedial measure can render the enemy ignorant of our disposition or intentions. The complexities of conducting ECCM on radars and other noncommunications electromagnetic systems during an attack are analogous to and as difficult as those just described for communication systems.

a. **Training.** Communications training is essential. As was noted in paragraph 2004, most of the measures included under the heading of good ECCM are the same as those included under the heading of good communications procedures. FMFM 3-3F, *Guide to Electromagnetic Interference Control* and FMFM 3-3E, *Radio Operator's Handbook*, are valuable training guides. They and other manuals can be issued to individuals for retention and study. FMFM 3-3E is equally applicable to communications and noncommunications systems. Some of the points which ECCM/communications training should cover are—

### 6002. Preventive ECCM

The preventive ECCM (also called preventive measures) are the most important ECCM. The enemy will probably conduct ECM activities in conjunction with some other tactical evolution. It is difficult enough

(1) Proper radio procedure (outlined in ACP-125). Their use reduces transmission time.

(2) Use of brevity codes. The use of brevity codes can be faster than plain voice. (Brevity codes are as unsecure as plain voice.) Brevity

codes understood by all must be used at all times. They can also be used on secure circuits to reduce transmission times.

(3) Use of physical signals such as aircraft rocking wings and arm-and-hand signals.

(4) Use of radio with the squelch off. Radios that are always used with the squelch on are subject to the squelch capture effect discussed earlier.

(5) Proper use of the communications-electronics operating instruction (CEOI).

**b. Planning.** During planning, the following should be done:

**(1) Combat Information/Intelligence**

(a) Determine disposition of known or suspected enemy EW units which could hamper the unit's communications capabilities.

(b) Maintain and update information about the enemy's SIGINT/EW capability.

**(2) System Design.** The careful consideration of the following points, while not always possible to implement, will enhance the effectiveness and efficiency of communications and noncommunications systems and reduce their vulnerability to enemy ESM and ECM efforts.

(a) Position emitters with an obstacle between them and suspected known enemy ESM/ECM units.

1 A soft target background, such as dry, wooded areas absorbs a portion of the emitted signal—thus reducing range.

2 A hard target, such as rocky terrain or wet trees, scatters the emitted signal—thus degrading accurate direction finding (DF).

(b) Make maximum use of horizontally polarized, directional antennas.

(c) Site antennas so adequate signal strength is provided to all stations on each given net.

(d) Check each communications installation to ensure that antenna heights are consistent with the distance required to communicate with friendly units.

(e) Ensure each antenna has the correct number of elements or is cut for the appropriate frequency for which it is intended to operate.

(f) Remote antennas and retransmission facilities to preclude a signature that indicates the command post location.

(g) Assign higher frequencies to high priority nets when operating a VHF/FM transceiver.

(h) Avoid clustering of antennas at remote sites.

(i) Consider remoting radios a minimum of 1,000 meters.

(j) Prepare an alternate routing plan for high priority circuits to ensure continuity of communications and ease of redirecting traffic.

(k) Make maximum use of COMSEC devices.

(l) Use cryptographic aids such as authentication and numerical encipher equipment.

(m) Design nets with a similar number of stations (uniformity), to avoid unique or distinguishing features of friendly communications network.

(n) Redistribute traffic to less heavily-used circuits when such circuits have slack periods.

(o) Use *free nets* as opposed to *directed nets* when the situation permits.

(p) Provide backup equipment in the event of primary equipment denial.

(q) Strict adherence to maintenance schedules for equipment calibration. This includes test equipment.

(r) Alternate communications means, including provision for and periodic exercise of—

1 Messengers, the most secure means, which should be designated down to the lowest unit level.

2 Wire, which should be installed and used to the maximum extent possible when the situation permits; e.g., when the situation is static.

3 Visual communications (e.g., hand signals, flags, and pyrotechnics) which should be preplanned and specified meanings contained in the CEOI and Communications Annex.

4 Sound communications, which are limited to use between small units in close proximity.

(s) Operate only at the power output level required to achieve emitter function.

(t) Timeshare radar coverage if equipment and terrain permit.

### (3) Emission Control (EMCON)

(a) Emission control is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security (OPSEC), detection by enemy sensors; to minimize mutual interference among friendly systems; and/or to execute a military deception plan. Also called **EMCON**. (Joint Pub 1-02)

(b) Commanders plan for and establish EMCONs so they can control the electromagnetic emission signature of their commands. EMCON can be used by all elements of the MAGTF. For example, aviation flight leaders must plan EMCON measures for their aircraft; e.g., identification friend or foe use, radars, and communications.

**c. Execution.** It is a well-worn but true statement that an ounce of prevention is worth a pound of cure. During combat operations everyone who uses or supervises the users of electronic emitters must ensure that the appropriate and prescribed procedures are followed. Military histories are filled with accounts of military successes and failures where the execution of emission activities were a critical factor. In the Battle of the Bulge, the Germans achieved surprise largely by prohibiting the transmission of information about the planned offensive over radios. And during WW II, the British broke the German enigma codes largely because the operators of the enigma machines violated basic communications security rules.

## 6003. Remedial ECCM

The remedial ECCM (also called remedial measures) listed below are to be taken by equipment operators when confronted with ECM. It must be noted that the enemy may often seek to conduct ECM operations so it appears that the problem is being caused by equipment malfunctions, terrain masking, interference from the radios of friendly units, etc. Conversely, what appears to be ECM may be the result of equipment malfunctions, terrain masking, or mutual interference between friendly units. The following is a generic checklist that may be used for communications emitters. Similar checklists can be developed for noncommunications electromagnetic equipment.

**a.** Ground or disconnect the receiver antenna. (If the interference persists it may be assumed that there is an equipment problem. Conversely, if it ceases you are encountering interference from an external source.)

**b.** Continue to operate and do not disclose the effect of the interference or jamming.

**c.** Reduce transmission speed.

**d.** Tune the receiver slightly (1 kHz) above or below the operating signal. (If the detuning causes a sharp drop in the intensity of the interfering signal, it may be assumed that the interference is the result of spot jamming.)

**e.** Increase the transmitter power (equipment dependent).

**f.** Selectively change equipment and antennas until the jamming or interference can be worked through.

**g.** A conscious effort must be made by electronic equipment installers to ensure that all possible

sources of self-interference are reduced (i.e., remote lines paralleling power cables, radio relay trunk lines terminating in the same terminal boxes with remote lines, etc.).

**h.** Reorient/relocate antenna.

**i.** If possible, change the mode of operation, (e.g., International Morse Code).

**j.** Transmit critical messages over several nets using the same date-time group.

**k.** Use alternate frequency (when directed by proper authority). (For communications systems this is executed at systems control (SYSCON) direction only.)

**l.** Prepare and send an MIJI report.

# Chapter 7

## Electronic Warfare Reports

### 7001. General

A reports system —

- Identifies what information is important.
- Identifies which headquarters and agencies need the information.
- Identifies which headquarters and agencies will report the information.
- States the format in which the information will be reported.
- Requires the submission of this information.

By identifying and requiring the reporting of important information as a matter of routine, a reports system frees the staff officers to attend to the extraordinary, rather than routine, situations.

### 7002. MIJI Reports

ECM techniques that an adversary tries and finds successful at one time and place will probably be used again until it becomes clear that we understand and are taking effective countermeasures against these techniques. Further, since (as was noted in paragraph 2003) some ECM techniques are subtle (i.e., leave the operator unaware that he is the victim of ECM), a worldwide view must be taken of aggressors' ECM activities. The MIJI report is the vehicle for reporting information that can be used by the JEWIC to (1) analyze incidents that might be caused by adversaries ECM and (2) determine effective countermeasures.

See MCO 3403.3, Meaconing, Interference, Jamming, and Intrusion, for detailed instruction on submitting MIJI reports.

### 7003. TERPES-Generated Reports

**a. General.** The TERPES is organic to VMAQ-2 and is used to analyze the data collected by EA-6Bs on enemy radar. It prints out the results of aircraft missions in four basic reports: the electronic reconnaissance intercept message (ERIM), the electronic reconnaissance intercept report (ERIR), the electronic reconnaissance mission analysis report (ERMAR), and an OPREP-4. Additionally, TERPES can provide EW reports in joint interoperability of tactical command and control systems (JINTACCS) formats. TERPES reports can also be generated to provide specific information in addition to that requested in the four basic reports listed above.

(1) **ERIM.** Is produced within 30 minutes of data collected by EA-6B being fed into the TERPES computer. It reports those radar transmitters which are high threat to the MAGTF.

(2) **ERIR.** Is produced within 1 hour of data collected by EA-6B being fed into the TERPES computer. It reports those radar transmitters which were not reported in the ERIM and are a threat to the MAGTF.

(3) **ERMAR.** Is produced within 3 hours of data collected by EA-6B being fed into the TERPES computer. It reports all hostile emitters which were not reported in the ERIM and ERIR.

(4) **OPREP-4.** Is produced within 3 hours of data collected by EA-6B being fed into the TERPES computer. It reports all hostile emitters and ECM performed by EA-6B.

(5) **JINTACCS.** Is produced within 3 hours of data collected being feed into the TERPES computer. It reports the same information as an OPREP-4 report.

(6) **Reports in Response to Requests for Specific Information.** Are produced at earliest opportunity based upon the relative priority of the report. Report format is specified by the requester.

**b. Classification.** All TERPES-generated reports are classified SECRET and are marked to be reviewed for declassification 20 years from the date they are produced.

**c. Distribution of TERPES Reports.** The TERPES-generated reports contain vital electronic intelligence. They should be sent directly to all units and headquarters which need the information. The shorter the delay between the mission and the receipt of the TERPES reports, the more valuable will be the reports to the recipients. The transmission of those reports to the S/EWCC for retransmission to other units and headquarters which need the information needlessly delays the receipt of this information by those headquarters.

**d. Formats.** TERPES-generated reports will be in the following format:

(1) **ERIM, ERIR, and ERMAR Reports.** (Only paragraphs A and B are used.)

(a) **Paragraph A.** Lists following items horizontally:

**1 Case Numbers.** A reference number which distinguishes each entry on a report. The same emitters can appear as different numbers on different reports.

**2 Type.** The type of emitter stated in standard ELINT notation.

**3 Freq.** The frequency on which the emitter was transmitting.

**4 Location of Emitter.** Given in latitude and longitude.

**5 Maj/Min/Orn.** Describes the ellipse within which the emitter is located. *Maj* is length of long axis in nautical miles. *Min* is width given in nautical miles. *Orn* is orientation of long axis in degrees.

**6 DF.** The number of direction finding fixes used to calculate the location of the emitters.

**7 Times (Z).** The period during which the fixes were made.

(b) **Paragraph B.** Gives remarks as appropriate.

(2) **OPREP-4.** (Only lines C, D, E, F, N, and Z are used.)

(a) **Paragraph C.** Lists objectives of mission.

(b) **Paragraph D.** Lists forces which participated in mission.

(c) **Paragraph E.** Gives route of aircraft which executed mission.

(d) **Paragraph F.** Gives specifics on ECM employed.

(e) **Paragraph N.** Lists emitters detected.

(f) **Paragraph Z.** Gives remarks to include but not limited to, aircraft configuration, status of equipment during mission, chaff dropped, and weather.

**e. Tasking of Emitters to Be Reported by ERIMs and ERIRs.** ERIMs and ERIRs report emitters which are a threat to the MAGTF. The aviation combat element will determine this based, in part, on its concept of air operations. In addition, however, the MAGTF headquarters should provide guidance on which emitters will be threats or high threats to the MAGTF.

**f. Action.** In preparation for the exercise or operation, the MAGTF headquarters will prepare taskings for ACE which—

- State which units and commanders are to be addressees on the TERPES-generated reports.
- State which radar emitters are to be reported on ERIMs and which on ERIRs.

## Chapter 8

# Employment of MAGTF Electronic Warfare Units With the Ground Combat Element

### 8001. General

Ground-based EW support to MAGTFs is provided by radio battalion or task-organized detachments, referred to as direct support units.

While a radio battalion and DSUs' primary mission is to provide SIGINT/EW support to the entire MAGTF, its assets, capabilities, and limitations are such that the GCE of that MAGTF is the principle recipient of the majority of the support provided by the DSU.

### 8002. Planning Considerations

Prior to the development of ESM and ECM plans, the following topics must be considered:

- Geographical characteristics of the area of operations.
- Mission and concept of operations of the supported unit.
- EEI/OIR.
- Enemy order of battle.
- Communications support requirements of the DSU.
- Logistical support requirements of the DSU.

### 8003. Employment Considerations

**a. General.** To provide for centralized control and coordination of EW assets, as well as ensuring

the integration of information collected through ESM with other intelligence information, radio battalion DSUs will be part of the SRIG (or detachment thereof) supporting the respective MAGTF.

While the primary role of the DSU is to provide EW support to the MAGTF commander, the DSU will normally be organized into two separate echelons. The first will be located with the MAGTF command element and consist of a headquarters element and an operation control and analysis (OCA) element. The second echelon will be forward deployed with elements of the GCE, consist of the majority of the DSUs' collection assets, and possibly will have a limited analytical capability.

**b. Support Relationships.** The support relationship which exists between the DSU and the MAGTF (or elements thereof) is established by the MAGTF commander.

**(1) General Support.** Requires the DSU to support the force as a whole. In a general support role, the DSU will remain under the immediate control of the force commander providing him with the flexibility to meet requirements of a variety of tactical situations. General support is the most centralized form of control and authority.

**(2) Direct Support.** Requires the DSU to establish liaison with the supported unit and coordinate all EW mission planning in direct response to the needs of that unit.

(3) **Attached.** A DSUs' assets are responsible for the conduct of both SIGINT and EW and these assets must be centrally controlled to ensure proper coordination and direction. As there will normally not be the required expertise or ability to provide adequate security provisions for the information required for in-depth analysis of collected information at lower levels of command, DSUs are seldom attached below division level for operational and/or mission control.

(4) If the MAGTF commander does not delegate any authority over elements of the DSU to the GCE commander via specific command and/or support relationships, DSU elements will normally be authorized to provide specific information and support to the GCE. This will normally be in the form of combat information and/or indications and warnings and will be specifically outlined in appendix 2 to annex B of applicable operations orders. Figure 1 summarizes operational and support relationships.

major headquarters and subordinate elements within the command. This is usually facilitated by locating the DSUs' command element with the MAGTF or GCE headquarters (depending on whether the support relationship established is general or direct support respectively).

Employment of the DSUs' collection assets are influenced by a number of considerations. As a general rule, in order for these assets to accomplish their mission in a satisfactory manner they will be forward deployed with (and in some cases in front of) elements of the GCE.

**a. DSU Operations in a General Support Role.** The electromagnetic battlefield cannot be divided into zones of action as can the physical battlefield. Electronic emissions do not respect unit boundaries nor do they follow specific paths. A signal may not be receivable 5 kilometers away but could be loud and clear 15 kilometers away in a slightly different direction. Terrain, frequencies, antenna patterns, and atmospherics can cause wide variables in the ability to conduct EW operations. To correctly identify, classify, and process EW information, these actions must be centrally controlled and coordinated.

A DSU in a general support role responds to the tasking of the force commander and supports the MAGTF as a whole. EW mission planning is

## 8004. Concepts of Employment

Regardless of the support relationship established, for the DSUs support to be effective provisions must be made for passing reports from the DSU to all

Support Relationship	GCE Submits Request to	DSU Establishes COMM w/GCE	DSU Establishes Permanent Liaison Element w/GCE	Responsible for Embark and Landing Plan	Responsible for Logistics	Security
General Support	MAGTF CE	No	No	MAGTF CE	MAGTF CE	DSU
Direct Support	DSU	Yes	Yes	GCE HQ	MAGTF CE	DSU
Attached	DSU	Yes	Yes	GCE HQ	GCE HQ	GCE

Figure 8-1. Support Relationships (Inherent Responsibilities).

accomplished in the MAGTF S/EWCC and coordinated by the DSUs' OCA element. All direction and tasking of DSU elements are carried out by the operational control and analysis center (OCAC) which will normally be located with the MAGTF command element.

In a general support role there is no inherent requirement for the DSU to make liaison or establish communications with any subordinate element of the MAGTF. When approved by the G-2/S-2 the S/EWCC may disseminate EW reports to elements of the MAGTF via the special intelligence communications system.

Figure 2 shows tasking and reporting chain for DSU in G-2 role.

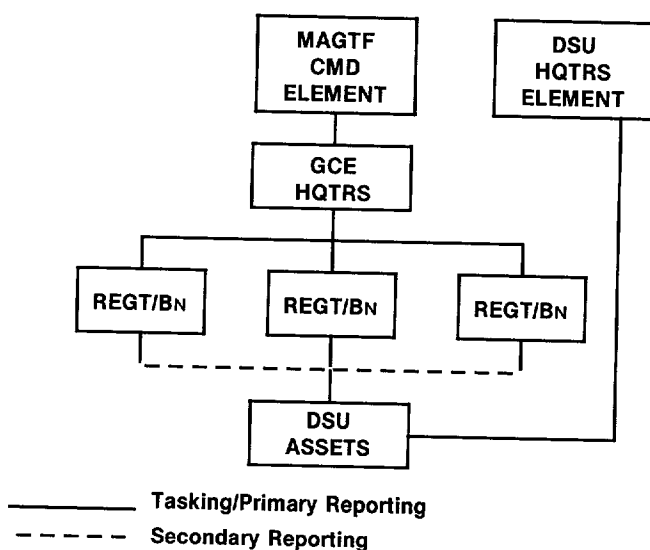


Figure 8-2. Reporting Chain (GS Role).

#### b. DSU Operations in a Direct Support Role.

A DSU in a direct support role responds directly to the tasking of the GCE commander. EW mission planning is accomplished in coordination with the GCEs' concept of operations. The DSU may establish the OCAC at the GCE headquarters or remain with the MAGTF command element. Regardless of the location of the OCAC, the DSU will ensure direct dissemination of combat information to the GCE commander.

In a direct support role, the DSU has an inherent requirement to make liaison and establish communications with the supported units (or subordinate elements thereof).

A DSU in a direct support role will establish a command/control element with the supported units' headquarters (and/or elements thereof). The purpose of this element is to conduct all mission planning in coordination with the concept of operations of the supported unit, disseminate combat information and coordinate the assets operating within the supported units' area of operations. These assets will include task-organized elements with DF, collection, and ECM equipment in various configurations.

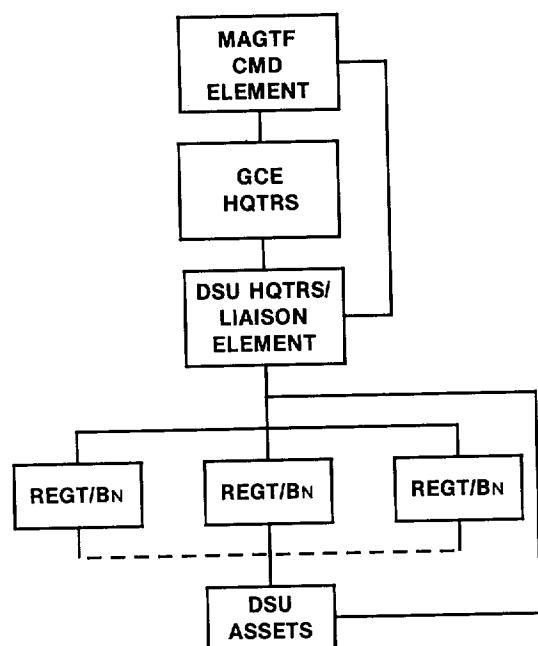
When establishing a direct support relationship, the following limitations should be established:

(1) Tasks accomplished for the supported unit shall also satisfy force-assigned missions. A direct support relationship does not preclude the DSU from responding to tasking generated by the MAGTF.

(2) Information provided to the supported unit in response to units' requests must also be provided to the MAGTF for further processing into intelligence.

(3) Direct support of ECM is permitted only on frequencies previously cleared by the MAGTF S/EWCC for preplanned missions. Any other requests for ECM will be submitted for approval to the MAGTF headquarters. When a DSU is operating in a direct support role, the support provided by the supported unit (and/or its subordinate elements) must be clearly defined prior to deployment of the DSU. The following should be considered when developing these requirements:

(a) Security requirements of the DSU—A limited firepower capability, consisting of individual and crew-served automatic weapons exists within the DSU. Additional security augmentation may be required from the supported unit.



———— Tasking/Primary Reporting

- - - - - Secondary Reporting

**Figure 8-3. Reporting Chain (DS Role).**

(b) Communications requirements of the DSU — The DSU will have the capability to establish internal voice circuits and terminal facilities for record communications. Communications paths for record traffic must be provided by the supported unit.

(c) Logistical requirements of the DSU — DSUs will normally include a logistical element capable of limited supply and maintenance efforts. Additional logistical support may be required from the supported unit in the form of consumable items such as POL, MRE , and batteries.

(d) Figure 3 shows tasking and reporting chain for DSU in direct support role.

## Chapter 9

# Electronic Warfare in Amphibious Operations

### 9001. Amphibious Operations Phases

This chapter discusses the basic electronic warfare considerations for amphibious operations. Detailed information in other publications is not repeated. See also Naval Warfare Publication (NWP) 10-1-40, *Electronic Warfare*.

In amphibious operations, an attack is planned by an amphibious task force (ATF) far from the AOA. Because of this separation, EW planners are faced with a number of problems which must be considered in arriving at an appropriate concept of support. The remainder of this paragraph outlines those considerations which occur in each of the five phases of the amphibious operation.

**a. Planning Phase.** During this phase, the emphasis is on developing the technical data base and on conducting ECCM necessary to provide OPSEC. Since the ATF and the landing force (LF) are far from the AOA, they must rely on national, theater, and other Services' assets for initial ESM support. As a result, ATF and LF EW planners must understand (1) the capabilities of these assets and (2) how to task them.

**b. Embarkation Phase.** During this phase, ESM support is still received from external agencies. By this stage the ATF and LF planners should have a fairly good data base and should be seeking very specific pieces of information in their taskings to ESM assets. ECCM is still important. OPSEC must be maintained to ensure the assault forces retain tactical surprise at the very least and strategic surprise if at all possible.

**c. Rehearsal Phase.** The data base continues to be built and ECCM continues to be important. In addition, EW equipment is checked. (Depending upon the location chosen for the rehearsal, OPSEC considerations may prevent the use of full power when checking jamming equipment.) Dummy loads may be required for electronic equipment checks rather than actually testing that equipment on the air.

**d. Movement to the Objective Area Phase.** As the ATF moves toward the objective area, its organic ESM assets will begin to detect enemy signals of interest. Marines will work with their Navy counterparts to conduct ESM operations in direct support of the ATF. In the initial stages of the movement, targets of interest will be enemy air and naval forces which could impede the ATF in its movement. As the ATF draws nearer to the AOA, enemy land forces and air forces which could oppose the LF become targets for ESM operations. The actual priority for any given ESM target will vary with the tactical situation, but, in general, those enemy forces posing a danger to the ATF as a whole will have to take priority over targets capable of interfering with the LF only. It should be obvious from the preceding discussion that Marine ESM operators must be conversant with opposing naval and air forces as well as land forces. Likewise Navy ESM operators must have an understanding of enemy ground forces so that they can support the landing force as required.

#### e. Assault Phase

(1) Enemy ECM should be expected during the assault when friendly forces are most vulnerable.

To minimize the potential of enemy interference being effective, electronic equipment operators must be well trained. The use of secure communications, brevity codes, terrain masking and other ECCM techniques, as well as minimizing reliance on radio communications through prior planning will all minimize the effectiveness of enemy ECM activity.

(2) ECM operations can be conducted to support the assault force. EA-6s will probably provide ECM support to strike aircraft. Ground forces could be supported by ECM activity. It may be possible to isolate enemy forces in the AOA with ECM operations. The U.S. Army may be capable of providing support during the initial stages of the assault. Marine planners must be aware of these Army capabilities and request any desired support in a timely manner. Once the radio battalion detachment lands it can begin conducting ECM.

(3) Until the radio battalion detachment is established ashore, the LF is dependent upon the ATF for its ESM support. This support is provided by Navy personnel working against ground force targets of interest. This requires not only prior training against ground-type communications, but also that the ATF personnel have a very clear understanding of the intelligence priorities of the LF. Close and continuing coordination between ATF and LF ESM planners is absolutely essential. But collection is not the only point to consider. In addition to ESM being provided by internal ATF assets, external agencies are still providing support. In all probability, there is far more ESM information available than can be passed to the assault force commanders over the limited communication links likely to be available. So in addition to their role in the production of ESM, shipboard personnel must select the information to be sent to commanders ashore. On the one hand, tactical commanders must not be inundated. On the other hand, they must receive all essential information. The G-2, in conjunction with the N-2, must determine which perishable information will be sent to

the MAGTF commander while forwarding the remaining information up the reporting chain to external units or laterally to other units. Integration of Navy and Marine cryptologic personnel from the beginning of the amphibious operation is the best method for ensuring the smoothest possible transition of ESM support from ship to shore.

(4) As part of advanced force or pre-assault operations, a radio reconnaissance team (RRT) may be inserted to provide EW support to the ATF. Dedicated, secure, OTH communications are required for RRT operations to be successful. The DSU, in coordination with RRT and other advance force reconnaissance elements, can establish a pre-assault jamming plan using hand emplaced, expendable jammers (HEXJAMS). The use of these assets has to be preplanned and relies on an extensive data base of the enemy communications.

## 9002. Responsibilities

### a. Commander, Amphibious Task Force (CATF)

(1) Develops the naval concept of EW and directs designated subordinate Navy commanders to prepare the necessary appendixes to support Navy forces.

(2) Directs subordinate Navy commanders to develop the necessary plans to support the landing force.

### b. Commander, Landing Force (CLF)

(1) Develops landing force concept of EW operations, and directs subordinate commanders to prepare the necessary appendixes to support the landing force.

(2) Determines and requests EW support required from Navy or other forces.

### 9003. Tasks During Planning

The following tasks are unique to electronic warfare in amphibious operations.

- a. Establish a single agency to control and coordinate ECM within the amphibious objective area (AOA).
- b. Develop criteria and procedures for passing forms of control applicable to EW from CATF to CLF.
- c. Develop plans for phasing EW equipment and personnel ashore.

### 9004. Planning Considerations

The following planning considerations are unique to electronic warfare in an amphibious operation:

- a. Continuity of friendly ESM/ECM efforts ashore and afloat during the initial stages of the assault.
- b. Limited technical data (e.g., frequencies or call signs) on the enemy within the AOA.
- c. Maintenance of adequate technical support for EW units ashore during the initial stages of the assault.

### 9005. Phasing of Electronic Warfare Personnel Ashore

There are several key officers the commander landing force should rely upon: the SIGINT officer, the OIC of the radio battalion detachment, and his assistant. The movement of these personnel ashore

should allow for the best utilization of their skills from an overall LF standpoint and should facilitate the passage of ESM information to the MAGTF commander. While not the only method for employing these personnel, the following is a starting point for considering their roles during the assault phase:

**a. EWO.** During the earlier phases of the operation this officer determines MAGTF ESM requirements and states those requirements to the radio battalion detachment, the ATF, and (when appropriate) to external agencies. He represents the MAGTF commander with the various ESM agencies. During the assault phase, he continues to be available to the MAGTF commander. Until the MAGTF commander moves ashore, the EWO coordinates LF requirements with ATF representatives on a face-to-face basis. He should move ashore with the MAGTF commander and then continue to serve as the commander's interface with ESM assets—both radio battalion assets ashore and ATF/external agencies offshore.

**b. Radio Battalion Detachment OIC.** He is responsible for converting MAGTF ESM requirements into technical ESM collection taskings. He is also responsible for supervising his detachment's personnel while they are integrated with the ATF's Navy ESM operators. Once the assault starts, he must move ashore relatively quick in order to assume control of his subordinates ashore. He must establish communications with the MAGTF commander (whether still afloat or ashore) in order to remain current in the MAGTF's ESM requirements and to provide necessary supporting reports. He must also ensure the rapid establishment of his detachment ashore to enhance the amount and timeliness of ESM support available to committed forces. The radio battalion detachment OIC may also act as the MAGTF SIGINT officer, as required.

**c. The Radio Battalion Detachment AOIC or Senior Enlisted.** Unlike the two previous individuals, this Marine will experience a significant expansion in his role during the assault phase

of the operation. Prior to the assault phase, he assists his OIC in determining technical collection requirements and supervising detachment personnel. When the OIC moves ashore to establish the radio battalion detachment and the SIGINT officer moves ashore to support the MAGTF commander, the AOIC should remain afloat to represent the LF's interests with the ATF in ESM matters. He must understand the scheme of maneuver well enough that he can convert requirements passed shore to ship by the MAGTF SIGINT officer into collection tasks for ATF Navy

personnel and/or external agencies. In essence, from the time other key ESM personnel begin moving ashore until the radio battalion detachment is fully established on the beach, he is responsible for coordinating ESM support to the MAGTF. To be successful in this role, he needs not only a good knowledge of his own field, but he must also be fully briefed on the MAGTF's concept of operation and must also understand fully the capabilities of Marine, ATF, national, theater, and other Service ESM assets and the means for requesting their employment.

# Chapter 10

## Electronic Threat

### 10001. General

It is important to protect ourselves from enemy EW. To do that, we must know our enemy. Because the Soviet threat is generally considered the most capable, the Soviet model is discussed in this section.

### 10002. Concepts

The basic Soviet concepts of EW are found in open military writings and are included under such general headings as reconnaissance, security, camouflage, and air defense. The discussions contained therein relate essentially to the three basic elements of Soviet counter-countermeasures, and electronic counter-countermeasures. Signals intelligence is employed both in intelligence collection and as a means of tactical reconnaissance to include targeting for artillery forces and airstrike. ECM are used to neutralize enemy communications and electronics through jamming or deception. ECCM capabilities in opposing forces are achieved through equipment redundancy, alternative subsystems, system design, operator skill, and strict enforcement of signal security. EW operations are closely coordinated with and support the combat operations plan. These operations may include jamming, electronic deception, camouflage, and nuisance intrusion.

### 10003. Electronic Countermeasures Threat

a. Soviet-trained technicians have an excellent grasp of the theory and practice of all phases of

EW. To what extent these concepts have been translated into deployed systems is only partially known, and probably will be apparent only with the outbreak of a major war.

b. Among the various EW means covered in Soviet technical writing are:

(1) Jamming in support of air defense operations to suppress radar bombing systems, radio navigation equipment, radio control links of air-to-surface missiles (ASMs), surface-to-surface missiles (SSMs), and radar jamming, including chaff, as camouflage of military targets.

(2) Jamming in support of ground operations to suppress enemy communications, electronic surveillance systems, and radio control links of surface-to-air missiles (SAMs), ASMs, and SSMs.

(3) Electronic reconnaissance, including electro-optic means, for the detection and location of enemy radar, CPs, communication centers, and nuclear delivery systems.

c. The principal systems discussed in detail are: radar jamming (barrage and spot noise, pulse, chaff, and decoys), electronic jamming of command guidance systems (pulse and simulation), and radio communications noise jamming of AM and FM signals.

## 10004. Electronic Warfare Capabilities

a. Knowledge of some Soviet-type EW capabilities is derived from the Arab use of Soviet EW equipment during the October 1973 Middle East War. It is unlikely that the systems observed represented the full panoply of EW systems available to Soviet forces, nor were they necessarily the most modern.

b. The EW means used by the Arabs against Israeli ground forces include:

- (1) SIGINT interception of the clear text radio communications of Israeli forces.
- (2) Direction finding of Israeli radio transmissions for targeting.
- (3) Barrage jamming to disrupt Israeli command channels.
- (4) Intrusion to give false directions and orders to Israeli units.

c. The Arab air defense system provided a forecast of the weaponry and ECCM of the Soviet forces. Their use displayed the following:

- (1) **ELINT Security.** The radars of the SAM and the anti-aircraft artillery, which were moved forward to cover the initial assault, were kept silent until after the initiation of the assault.
- (2) **Frequency Diversity.** The ability of the tracking and guidance radars to change frequencies to overcome jamming.
- (3) **Multiple and Interchangeable Guidance.** Some systems worked on pulsed radar, others on continuous wave. The radar tracking systems also possessed optical tracking for continued operations in a high ECM environment. Other systems were infrared homing.

(4) **Mobility.** All tactical air defense systems were extremely mobile and capable of quick change of position after firing or being spotted by reconnaissance.

## 10005. Tactical Reconnaissance

Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (Joint Pub 1-02) It is the most important form of combat support action. The Soviets recognize that in order to make the maximum use of their massed firepower and mobility potential for rapid armored advances, their target acquisition capabilities must be characterized by accuracy and short reaction time. Tactical reconnaissance is conducted to varying depths by reconnaissance units and by all other troop units. Troop units are particularly concerned with those enemy activities that affect their particular mission or purpose.

a. **Air Reconnaissance.** This is one of the principal sources of combat intelligence and is undertaken by elements of the tactical air army which is tasked by the Front headquarters. These aircraft have visual, photo, infrared, radar, and SIGINT capabilities. Reconnaissance aircraft, in general, carry weapons and are capable of carrying out ground attacks on targets of opportunity. A certain proportion of reconnaissance missions is accomplished by pairs of aircraft assigned search and destroy missions. These missions are particularly directed against enemy nuclear delivery means. These missions will be flown by attack aircraft.

### b. Electronic Intercept and Direction Finding

(1) **Intercept.** As demonstrated by Egyptian use of Soviet equipment during the October 1973 Middle East War, the Soviets have an extensive intercept capability for both radio

and radar. Intercept units are moved forward immediately behind leading regiments and have the capability to intercept all enemy transmissions within the following distances from the forward edge of the battle area (FEBA). These ranges are extended greatly when airborne intercept equipment is used:

- Artillery ground radar: About 25 kilometers.
- VHF: About 40 kilometers.
- HF ground waves: About 80 kilometers.
- HF skywave: Unlimited.

**(2) Direction Finding.** The Soviet direction finding capability is equivalent to that for intercept.

### **(3) Reaction Time**

**(a)** Information derived from the intercept of *clear* traffic is evaluated and acted upon quickly.

**(b)** While information from DF is evaluated quickly, it is unlikely to provide a sufficiently accurate fix for identification of a moving, point-type tactical target. If a nuclear strike is required, confirmation is most likely accomplished by aerial reconnaissance and at least 2 to 2½ hours might elapse from initial electronic intercept before a strike is launched. Information of an extremely perishable nature on targets within conventional artillery range, such as forward command and control facilities and unit command posts (CPs), is usually reacted on as an immediate fire mission (target of opportunity).

**(4)** Artillery target acquisition and reconnaissance. Front, army, and divisional artillery units have an organic target acquisition capability. Generally, these units contain:

- Surveillance and weapon-locating radars.
- Radar intercept/direction finding sets.

- Sound ranging out to about 14 kilometers from the FEBA.
- Flash spotting observation posts (OPs).

## **10006. Radioelectronic Combat**

**a. General.** Radioelectronic combat (REC) is the Soviet plan for accomplishing and integrating SIGINT, target acquisition, ECM/ESM, electronically-supported firepower, and ECCM. The essence of REC lies in a planned sequence of activities that attempt to selectively deprive Soviet adversaries of control of the tactical electromagnetic environment. REC is used to support Soviet tactical objectives, including use in both offensive and defensive operations.

**(1)** The enemy attempts to find the communications *keystones* upon which the command and control of U.S. tactical forces and weapons systems are dependent.

**(2)** As *keystones* are developed by enemy intelligence, they are prioritized according to their expected relative impact on the battle. The enemy intent is to identify and prioritize the U.S. control centers so that they may be destroyed or jammed.

**b. Priorities.** REC target priorities are generally as follows (these priorities will change as the tactical situation develops and are dependent on the level of command):

- Artillery, missile, and air force units that possess nuclear capabilities, and their associated control systems.
- CPs, OPs, radio centers, and radar stations.
- Field artillery, tactical air, and air defense units limited to conventional firepower.
- Reserve forces and logistic centers.
- Point targets that may jeopardize advancing enemy forces.

### c. Planning

(1) The systematic physical destruction by firepower of U.S. control points and electronic equipment is an integral part of REC planning.

(2) During combat operations, the enemy electronic reconnaissance and intelligence effort is devoted to continually locating those friendly control points that are the greatest detriment to enemy forces at any given time.

### d. Conduct

(1) The enemy realizes that it does little good to disrupt the communication links from battalion to regiment unless the data being transmitted on the nets is so *time valuable* to U.S. forces that its disruption will enhance the enemy effort. Accordingly, the primary mission of REC becomes the identification and location of these control points for targeting purposes at a time of greatest benefit to the enemy. At the appropriate time during the engagement, usually in conjunction with Soviet unit maneuvers, MAGTF communication and control systems will be targeted for destruction by Soviet fire or disruption by a variety of ECM techniques.

(2) To locate U.S. electronic transmitters, the enemy employs direction finding in conjunction with other information to provide targets for enemy suppressive fires and jamming. Direction finding of radio transmitters from ground DF stations is usually not precise over long distances. Airborne DF and close-in ground DF do provide sufficiently accurate locations for the enemy's suppressive artillery fires, particularly his area weapons system like the multiple rocket launcher (MRL).

(3) Due to the high concentration and wide dispersal of MRL fires, they can be delivered against soft targets located by direction finding with a high probability of destroying the target. Since radars can more accurately be located by direction finding, suppressive fires are effective against them.

(4) Because of the length of their transmissions, the peculiarity of their signal and power output, jammers are easily located and identified as targets for attack by suppressive fires. For other transmitters the enemy requires information from other sources to convert DF locations into targets. In many instances, this information is provided by poor signal security or poor ECCM on the part of our forces.

(5) The enemy's success in conducting radio and radar DF against friendly emissions will largely determine the amount of command and control and weapons control systems which friendly forces will have to fight the war.

(6) Radio direction finding (RDF) and intercept are the core of REC success. Without emitter locations, SIGINT, jamming, and targeting are severely degraded. This RDF capability becomes the target of friendly counter-REC actions. Most of the enemy tactical RDF and intercept equipment is mobile and transportable. Some aircraft in the tactical air army, as well as support aircraft from higher echelons, are equipped for DF and intercept operations.

(7) Another function of REC is to counter the success U.S. forces may have with their targeting or target acquisition means which must be disrupted to disallow its effectiveness. REC has the responsibility to deny U.S. intelligence insight into enemy plans for future operations.

(8) As the battle proceeds, REC is expected to begin massive jamming of low-level FM nets to deny command and control of U.S. maneuver units. The enemy's intent is to slow the battle and defeat our forces in detail. Armor units may be particularly vulnerable when they are denied communications due to jamming, especially when under enemy artillery fires that cause them to *button up*.

(9) The REC capability is real; it demands attention in the development of an opposing battle plan.

**e. Signals Intelligence Threat.** The Soviet view of signals intelligence includes the U.S. concept of both SIGINT and ESM. Radio direction finding is used to—

(1) Provide approximate locations of electronic emitters that can then be fired on by artillery barrages or multiple rocket fires.

(2) Provide suitable locations for firing on most radars and jammers.

(3) Provide locations which, when applied in conjunction with signal and terrain analysis, can be refined to a target area of sufficient accuracy for artillery fires.

(4) Build a picture of the battlefield which shows the disposition and reveals the intentions of our units. The dispositions and intentions of units may be revealed by a single key emitter.

**f. Radiomas Kirova: Wartime Reserve Modes.**

(1) Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that (a) will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but (b) could be exploited or neutralized if known in advance. **Wartime reserve modes** are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. Also called **WARM**. (Joint Pub 1-02)

(2) Since 1965, the Soviets have developed and exported a WARM capability in all their electronically-dependent systems. WARM serves as an effective ECCM, as it renders useless a history-based EOB.

(3) Soviet doctrine is to employ WARM as hostilities commence to support their overall

deception plan and to assist in the accomplishment of their REC objectives.

(4) Commanders must be aware of the possibility of every WARM employment, and staff EWOs must devise plans for alternate means of identification and countering enemy emitters when WARM-rendering conventional ESM ineffective.

(5) EW programming of friendly systems must be continually updated to reflect the most current WARM parameters.

## 10007. Complementary Roles of RDF and Intercept

a. Electronic emitters can be used to identify units, weapons, and command posts because unit identity can be simply determined by one or a combination of—

- Plain text revelation.
- Type transmitter.
- Call sign peculiarity.
- Analysis of communications traffic.
- Transmitter modulation.
- Operator identification.
- Duration and frequency of messages.
- Analysis of unauthorized codes or ciphers.
- Misuse of authorized call signs, codes, or ciphers.

b. All of this is used in conjunction with an analysis of the general location of a unit on the battlefield provided by direction finding.

c. A radio signal provides information even when protected by code or cipher.

d. Electronic emitters can provide the enemy with the detection, general location, and possible identity of the unit which they serve.

## **10008. Complementary Roles of RDF and ECM**

Efficient jamming is enhanced when DF is used to select and generally locate enemy communications nets. The receivers of the target radio net are then selected for jamming, and the jammer's antenna oriented to the location reported by RDF. Enemy doctrine establishes a requirement to jam U.S. command, control, and weapons system communications when they cannot be destroyed by suppressive artillery fires. Enemy forces jam VHF, but they also

depend on VHF for their own command, control, and weapons systems. One way they are able to control this problem is using VHF directional antennas which have a greater effective radiated power for their own communications. They practice this technique in training. The Soviet-type force uses VHF and UHF multichannel communications at selected key levels and employs HF tactical communications as a redundant communications system down to tank platoon level.

Jamming can also support direction finding by jamming a target for a prolonged period and causing the target station to backlog traffic. When the jamming is terminated, the target station may then transmit continuously over a long period to relieve the backlog of traffic. Prolonged transmission in these cases enables direction finding to refine numerous bearings obtained during the long transmit time.

# Appendix A

## Graphic Formats and Color Coding

1. A collateral map and a strategic map will be maintained (usually in the S/EWCC) that presents an up-to-date display of the enemy and friendly situation. The enemy situation will be presented in red, and the friendly situation will be presented in black.

2. SIGINT information will be displayed on a SIGINT map. Enemy EOB information will be color coded using appropriate symbols.

**Black**—early warning radar sites.

**Green**—ground control intercept sites.

**Orange**—antiaircraft fire control radars.

**Red**—SAM guidance radars.

**Yellow**—SSM guidance radars.

**Blue**—navigational and precision-approach radars.

**Brown**—commercial installations.

3. This appendix does not include all communications-electronics symbols required for general use in the S/EWCC. Special symbols used in communications diagrams, line route maps, traffic diagrams, and communications operations maps are contained in FM 21-31. In addition, the following symbols may be combined with other military symbols or may be further annotated to show their detailed function and type.

### a. EW equipment and units:

- EW unit

- Radio Direction Finder Station  
(Indicate frequency range)
- Radio Intercept/Monitoring Station  
(Indicate frequency range)
- Radio Relay Intercept Station  
(Indicate frequency range)
- Radar Intercept and DF Station  
(Indicate frequency band—A/B/C/D . . . M)
- Jamming Station (Radio)  
(Indicate frequency range)
- Jamming Station (Radar)  
(Indicate frequency band)

### b. EW Targets:

- Radio Station  
(Indicate frequency range)
- Radio Relay Station (Terminal)  
(Indicate frequency range)
- Radio Relay Station  
(Indicate frequency range)
- Electronic Navigational Aid
- Radar Station  
(Indicate frequency band)
- Guided Missile  
(Indicate type—SSM/ASM/SAM)
- Operations Van (Comm)
- Cryptography Center

## Appendix B

# Joint Tactical Electronic Warfare Request Form

JOINT TACTICAL ELECTRONIC WARFARE REQUEST FORM  
(Electronic Warfare Support Measures/Electronic Countermeasures Missions)

A	Request # 1. <input type="checkbox"/> Precedence 2. <input type="checkbox"/> Priority	FROM
		TO
B	MAP REFERENCE: Producer 1. AMS 2. ACIC 3. NAVOCEANO 4. Other (specify) _____ Series _____ Date _____	<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved
	TYPE EW MISSION SUPPORT REQUESTED: <input type="checkbox"/> 1 ESM <input type="checkbox"/> 2 ECM <input type="checkbox"/> 3 Combination	By/Reason
D	MISSION TO BE SUPPORTED (DESCRIBE): 1. Nature of Mission: _____ 2. Route of Travel (*Altitudes): _____ 3. Timing: _____ 4. Force Size: _____	SENT TIME BY
		RECEIVED TIME BY
		CHECKED BY
		ACKNOWLEDGED
E	ESTIMATED THREAT TO EW SUPPORT MISSION: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ 6. _____ 7. _____ 8. _____ 9. _____	
F	ESTIMATED EOB TO AFFECT MISSION: (Type, Electronic Frequencies, Location)	1) _____ 2) _____ 3) _____ 4) _____
G	DESIRED RESULTS: 1. <u>ESM</u> a. Area Search _____ b. Specific Search _____ 2. <u>ECM</u> _____	
H	COORDINATING INSTRUCTIONS: 1. *Mission Rendezvous _____ 2. Mission Contact (C/S, Freqs): a. Primary: _____ b. Secondary: _____ 3. Friendly Force(s) Possibly Affected: a. Unit(s): _____ b. Address: _____	COORDINATION 1) _____ 2) _____ 3) _____ 4) _____

\* Applicable or when known.

I	REPORTS: 1. INFLTRPT C/S_____ FREQ_____	COORDINATED
	2. MISREP _____ 3. TESM _____ 4. Other _____	
J	REMARKS/SPECIAL INSTRUCTIONS: <input type="checkbox"/> JAMMING FREQ RESTRICTIONS	<input type="checkbox"/> Artillery <input type="checkbox"/> AIR DEF <input type="checkbox"/> AVN <input type="checkbox"/> NGF
K	1. RESTRICTIVE FIRE/AIR PLAN 2. IN EFFECT Requesting Unit <input type="checkbox"/> IS NOT <input type="checkbox"/> NUMBER <input type="checkbox"/> (from time) _____ <input type="checkbox"/> (to time) _____	Notified By DTG
	3. LOCATION 4. WIDTH (Meters) <input type="checkbox"/> (From – coordinates) <input type="checkbox"/> (To – coordinates)	By  <input type="checkbox"/> Accept <input type="checkbox"/> Refuse
	5. ALTITUDE/VERTEX <input type="checkbox"/> (Maximum/VERTEX) <input type="checkbox"/> (Minimum)	REASON

AIR MISSION DATA			
L	1. MISSION NO	2. AIRCRAFT C/S	3. NO/TYPE ACFT
	4. EST/ACT TAKEOFF		5. RENDEZVOUS (Coord/NavFix)
	6. MISSION CONTACT C/S _____ Freq _____		7. MISSION TIMING TOT _____ Duration _____
	8. ESM <input type="checkbox"/> Area of Search <input type="checkbox"/> Signals to be Searched		
	9. ECM <input type="checkbox"/> Profile: _____ _____ _____  <input type="checkbox"/> Type Signals/Freqs for ECM: _____ <input type="checkbox"/> Chaff/Decoy Drop: _____		
	10. INFLT RPT C/S _____ Freq _____		11. RESTRICTIVE FIRE/AIR PLAN (BLOCK K)
	12. REMARKS		

NOTE: Joint Pub 12, Tactical Command and Control Procedures for Joint Operations, has instruction on the proper completion of this form. (See also FMFM 5-10, Air Reconnaissance.)

Explanatory Notes

NOTE: This form combines both electronic warfare support measures (ESM) and electronic countermeasures (ECM) request requirements. It will therefore not always be appropriate to complete every line item. The requestor should complete as many line items as he has information for, regardless of the type mission requested.

Title and Element(s)		Explanation
Line A		
Request Number		As directed.
1.	Precedence	Indicate the requester's assignment relative to his other requests stated numerically in descending order of importance.
2.	Priority	Use numerical designation below to define the tactical situation.
<u>Priority No.</u>	<u>Priority</u>	<u>Definition</u>
1	Emergency	Targets which require immediate action and precedence over all other categories of mission priority.
2	Priority	Targets which require immediate action and take precedence over routine targets.
3	Routine	Targets of opportunity, targets which do not demand urgency in execution.
Line B		Self-explanatory.
Line C		Self-explanatory.
Line D		
Mission to be Supported		Describe, in sufficient detail, the profile and specifics of the mission needing support. The amount and type of support will be determined, to a large extent, from the information provided here.
Line E		
Estimated Threat to Mission		List the known and suspected enemy order of battle that will probably affect the mission to be supported.
Line F		Self-explanatory.

Title and Element(s)	Explanation
<b>Line G</b>	
Desired Results	Describe the objectives of the requested support.
1. ESM	Include EEI that collection is responding to. When requesting Specific Search, provide EEI on emitter to be collected on; i.e., radio frequency, pulse repetition frequency, pulse duration, scan type, scan duration/rate, and other significant information.
2. ECM	Designate specific electronic countermeasure effects desired in relation to Lines E and F when applicable. Identify frequencies to be affected when they are known. Tactics and employment methods may be recommended.
<b>Line H</b>	
Coordinating Instructions	
1. Mission Rendezvous	Designate by coordinates or navigation system fix when mission requires inflight rendezvous.
2. Mission Contact	List the call sign(s) and communication frequencies for the supported agency to be contacted by mission aircraft when contact is necessary.
3. Friendly Force(s) Possibly Affected	If there is a chance that the effects of the requested mission will interfere with other operations, provide information on the units that may be affected; to include description of interference when known.
<b>Line I</b>	Self-explanatory.
<b>Line J</b>	Self-explanatory.
<b>Line K</b>	
1. Restrictive Fire/Air Plan	Safety measures for EW support mission. The restrictive fire plan establishes airspace/surface area that is reasonably safe from friendly, surface-delivered, non-nuclear fires. The restrictive air plan provides a warning to aircraft of the parameters of surface-delivered fire in a specific area. A plan number is issued, as appropriate. The plan should be identified as <i>Fire</i> or <i>Air</i> .
A. Is not	
B. Number	
2. In Effect	Establishes the time period that the applicable plan will be in effect.
A. From time	
B. To time	

Title and Element(s)	Explanation
3. Location	
A. From—coordinates	Military grid coordinates by bearings and distances from a known navigation aid.
B. To—coordinates	
4. Width (meters)	From either side of the centerline defined by the above coordinates. (May not apply to the restrictive air plan.)
5. Altitude/VERTEX	Use subitem A for VERTEX only entry.
A. Maximum/VERTEX	Given in mean sea level (MSL) altitude; altitude above sea level.
B. Mimimum	

**Line L**

(To be filled out by mission tasking agency)	Self-explanatory.
---	-------------------

**ACTIONS COLUMN ALONG RIGHT EDGE**

APPROVED/DISAPPROVED	Indicate approval action by requester.
SENT	Initials of sender and time sent.
RECEIVED	Initials of receiver and time received.
CHECKED BY	Indicate agencies (persons) having reviewed the request after receipt. This may lead to further action requiring use of top blocks by higher echelon.
ACKNOWLEDGED	Use as locally directed or as necessary.
COORDINATION/COORDINATED	Self-explanatory.
REQUESTING UNIT NOTIFIED BY	Indicate person who received approved request and time received. Indicate whether or not mission will be tasked and reason for refusal.

# Appendix C

## Electronic Jamming

### 1. General

This appendix discusses electronic jamming. It is intended as background information for those who are not electronic warfare specialists. If one understands how jamming is done, one can better avoid it, reduce its effectiveness, and understand what it can do for you.

Electronic jamming was first used against radio communications to obliterate or overpower the enemy transmission, or to so irritate the radio operator that he could not do an efficient job. This *brute force* approach to electronic jamming required comparatively simple modulations, but the approach instantly alerted the enemy operator to the jamming effort. While *brute force* jamming is still widely used today, more sophisticated modulations and techniques are available which permit disruption of transmission without immediately alerting the enemy operator that his transmissions are under attack. These sophisticated techniques are used for, among other purposes, causing operators to stop using communications security equipment (by breaking synchronization) or reducing communication equipment availability by making it appear that the equipment is malfunctioning.

### 2. Radiation Jamming

Radiation jamming involves those equipments and devices that radiate electromagnetic energy and employs one of the following techniques:

**a. Barrage Jamming.** Barrage jamming is the simultaneous jamming of a number of adjacent channels or frequencies. The barrage jammer transmits electromagnetic energy over a broad

band of frequencies to mask a large portion of the electromagnetic spectrum. It is capable of simultaneously jamming all receivers within the bandwidth of the jamming signal. The effectiveness of the barrage jammer in masking a strong electromagnetic signal is limited, due to the power spread over the range of frequencies involved. Effective barrage jamming requires a high power emitter. This type of jamming should not be used in frequency bands used by friendly forces, except when previously coordinated, so as to eliminate friendly interference.

**b. Spot Jamming.** Spot jamming is the jamming of a specific channel or frequency. This is the most common form of jamming because it causes minimum interference with friendly emitters and permits maximum use of available power. There are several types of spot jammers including manual spot, multiple spot, and sequential spot.

**(1) Manual Spot Jammers.** These jammers require the operator to initially position the jamming signal over the signal to be jammed and to retune as the signal changes frequency or new targets are engaged.

**(2) Multiple Spot Jammers.** Employ a number of narrowband transmitting devices in one equipment assemblage and can simultaneously spot jam a number of different frequencies on a power sharing basis. When a signal which falls within one of the narrowband frequencies is received, the jammer automatically concentrates all power on that frequency spot. When another signal appears on another frequency spot, the jamming power is split and both frequency spots are jammed. As more signals appear within the frequency range of

these narrowbands, the jamming power continues to split and is thus reduced on any one particular signal.

**(3) Sequential Spot Jammers (or Sweep).** Can jam a number of different frequencies in rapid succession. Each frequency jammed receives the full power output of the jammer for a short period of time.

### 3. Reradiation Jamming

Jamming by reradiation is accomplished by receiver-transmitter assemblies. The more common usage of these configurations in an electronic deception role is covered later. When used in a jamming role, repeaters and transponders are essentially automated jammers.

**a. Repeaters.** Intercept the victim signal, alter it in some fashion, amplify the altered version, and retransmit it for the purpose of disrupting or falsifying the information transmitted to the victim receiver. Repeater applications for jamming and deception are generally limited only by the state of the electronic technology and the ingenuity of the individual in devising methods for altering the intercepted signal. Delaying retransmission of the intercepted signal will produce an unintelligible output from any electronic system receiving both the original and altered versions of the signal.

**b. Transponders.** Automatically transmit a predetermined signal when programmed to respond to specific types of victim signals.

### 4. Reflection Jamming

Reflection jamming is normally used to confuse enemy electronic systems. Reflective devices such as chaff, rope, and corner reflectors provide enemy electronic systems with false targets and thereby degrade their effective operation.

**a. Chaff.** Consists of narrow metallic strips, of various lengths and frequency responses, used to reflect echoes to the receiving components of the radars. Chaff, sometimes call window, reflects a

signal which appears on a radar scope as a series of spaced echoes or as one of continuously lengthening target indications. The expansion of the echo on a radar display is due to the dispersion of the chaff after launching.

**b. Rope.** A form of chaff consisting of a long roll of metallic foil or wire designed for broad, low-frequency response. The echo reflected by rope appears on a radar scope as a single target or a formation of targets.

**c. Corner Reflectors.** Consist of flat reflecting surfaces connected to form a three-dimensional reflector. The reflector may be produced in a variety of shapes, including cubes, diamonds, and pyramids. Because of its electromagnetic reflective efficiency, the corner reflector appears on a radar as a much larger target. When rotated, the reflector appears as a moving target.

### 5. Type of Jamming Signals

A signal is transmitted for the purpose of jamming electronic emitters. The signal may be varied in amplitude, frequency, or pulse by an almost unlimited variety of modulating signals. The type of signal used in any given situation is determined by the capabilities of the jamming equipment, nature of the target, and desired results. Specific equipment and techniques are developed on a continuing basis to deal with particular threats. The equipment and techniques to be employed are many and varied. Equipment specifically designed for jamming would be most desirable to produce the best possible results. However, any piece of equipment that will radiate on the desired frequency may be a jammer. Common types are—

- Random noise.
- Babbled voice.
- Random keyed.
- Random keyed continuous wave (CW).
- Keyed CW.
- Modulated CW.
- Stepped tones.

## 6. Technical Effectiveness of Jamming

The technical effectiveness of a jamming system refers to its ability to achieve a particular ratio of jamming signal strength to transmitter signal strength at the target receiver. The information presented in this section is intended to provide general criteria for effectiveness assessment.

### a. Communications Jamming

(1) Considerations of availability of alternate communications and effect of jamming upon the tactical situation are normally deferred until the technical effectiveness of the system is assessed. Once the jamming system has been determined to have the potential to be technically effective, these considerations become germane to the problem.

(2) It is extremely difficult to identify a precise point at which jamming becomes effective; however, to facilitate the assessment, the concept of a *jamming threshold* has been developed. A jamming threshold is the jamming-to-signal ratio (JSR) above which a specific receiver type is considered to be effectively jammed. The actual calculation of this ratio is a complicated problem and is not a doctrinal matter.

(3) The technical characteristics, orientation, and location of both the jamming and receiving antennas strongly influence jamming effectiveness. Careful consideration of the following factors can result in significant improvement in the technical effectiveness.

(a) **Tuning.** Careful tuning of the transmitter and the antenna can maximize the transfer of RF power from the transmitter.

(b) **Use of Directional Antennas.** Whenever possible, the antenna should be made as direct as possible. This not only increases jamming effectiveness, but it also reduces interference with friendly electronic systems.

(c) **Polarization.** The transmitting antenna of an ECM device should be polarized in the same plane as the receiving antenna of the

intended victim receiver to obtain maximum effectiveness.

(d) **Elevation.** Antenna elevation may significantly reduce the propagation loss between the jammer and the target receiver and thus greatly increase the jammer signal strength at the receiver.

(e) **Soil Characteristics.** The electrical characteristics of the soil effect the gain realizable from an antenna.

(f) **Line of Sight**

(g) **Range**

### b. Noncommunications Jamming

(1) The assessment of the technical effectiveness of noncommunications jamming is an extremely complicated task. The large number of variables involved makes timely and accurate input essential for an accurate assessment.

(2) One of the more important variables is the physical size of the target. The larger the target, the more energy reflected, and, consequently, the more difficult the jamming problem. Except in the case of airborne ESM/ECM, it is difficult to assess with any accuracy the strength of the reflected signal. The target cross-section area will vary with changes in altitude with respect to the radar antenna.

(3) The *brute force* approach in which the jamming signal seeks to obscure the target through overpowering amounts of energy frequently is abandoned for more sophisticated low power approaches. The *gate stealing* techniques used against tracking radars is typical. In this approach, the average power merely has to exceed the average radar echo in order to be successful.

(4) In electronic jamming, the ability and training of the operator is critically important. His capability to make fine distinctions based on anticipated reactions and past experience is a key factor in any jamming or deception operation.

## 7. Noncommunications Jamming Techniques

**a. Barrage Noise.** Barrage jamming is intended to cover a broad frequency spectrum that includes the tuning spectrum of the target systems of a certain category.

**b. Fast-Swept Noise.** In order to be able to generate barrage jamming over a wide frequency spectrum with smaller transmitter power, narrowband jamming transmitters are built. At a high rate of speed, the narrow frequency band of this transmitter sweeps the complete operating spectrum of the target electronic systems.

**c. Spot Noise.** Narrowband jamming is produced in a relatively narrow frequency band which corresponds approximately to the bandwidth of the target receiver. The jamming transmitter must be tuned exactly to the operating frequency of the target system if narrowband jamming is to be fully effective.

**d. Fast-Acquisition Spot Noise.** Since the frequencies of electronic systems may be changed very rapidly while the frequency of a narrowband jamming signal must not deviate from the target receiver frequency by more than half a bandwidth, these jamming transmitters require complicated tuning and automatic frequency control devices.

**e. False Targets.** On the scope of a *radar system responder*, jamming is seen as a multitude of flickering spurious targets that resemble true targets. On the scope of the radar station, pulsed jamming signals will simulate real targets. The spurious response signals should not differ from the signals of the target system with respect to the structure of their spectrum, duration, and shape. In order to achieve optimum similarity between jamming pulses and real target pulses, the jamming pulses may be modulated in addition so that their marks on the scope will fluctuate like the

marks of real targets. On radar screens, instead of a clear and definite picture of the real air situation, there will be marks seen from false targets and even whole sectors and bands created from active and passive interference. If the pulse repetition frequency of the suppressed radar is constant, and the memory time of the carrier frequency in the frequency memory is considerably longer than the duration of the main pulse ( $t + r$ ), then it is possible to create, on the radar screen, false marks both lagging with respect to the target and leading the mark from the target. Interference constitutes one (or several) radio pulses radiated in answer to the received signal of the suppressed radar with a certain delay  $dt_3/dt$  corresponds to the speed of flight of the simulated target; the delay time is selected comparatively long. With quite high power of the jamming transmitter owing to the influence through lateral lobes on the screen of the suppressed radar, several false marks are created which move at a definite speed, which considerably complicates the work of the operators and can lead to erroneous actions of responsible persons of the anti-aircraft defense system of the enemy.

**f. Multiple Synchronous Pulse Interference.** The interference constitutes a series of radio pulses radiated in answer to the accepted signal of the suppressed radar. Radio interference pulses must correspond in form, duration, and power to radio pulses of reflected signals received by the pulse trains and should be identical with the repetition frequency of the main pulses of the suppressed radar. Otherwise, the enemy is able, by applying certain methods of selection, rather simply to be liberated from the interfering signals.

**g. Random-Pulse Interference.** Interference constitutes a sequence of radio pulses the basic parameters of which (repetition frequency, duration, and amplitude) are changed according to the random law. Random-pulse interferences are similar in their properties to interference obtained as a result of amplitude modulation of the carrier by limited noise.

**h. Conical-Scan Inverse Gain.** It is clear that interference of the examined form in its effect is equivalent to a certain fictitious target, not coinciding in space with true target. In other words, the interference signal generates false information, simulating the appearance of a second fictitious target whose angular coordinates differ from those of the true target.

**i. Range-Gate Capture.** In modern target tracking radar systems the receiver is keyed open only for a short period by a stroboscopic pulse after the target is acquired. The position of this stroboscopic pulse shifts in agreement with target range. In order to jam such a system, the first jamming pulses must be radiated with a time lag of  $t = 0$ . Gradually increasing time lag between target pulse and jamming pulse will cause the stroboscopic pulse to run away from the target. Again, turning the jammer off will cause the target to be lost.

**j. Velocity-Gate Stealer.** In a similar manner the operation of an automatic target tracking system is jammed with respect to target velocity. A change in target velocity is simulated by changing the jamming signal frequency. As a result, the gating pulse for target tracking with respect to target speed is deflected by the Doppler frequency

of the target signal. Subsequently, the emission of spurious signals is terminated. Every time, after deflection of the radar system by jamming signals, the operators must start a target search, from the beginning before the system can be switched to *target tracking* again.

**k. Swept Conical-Scan Inverse Gain.** Swept conical-scan inverse gain is the amplitude modulation of a carrier by sinusoidal voltage whose frequency is changed systematically in the range of possible scanning frequencies (sweep-through jamming).

**l. Expendable Jammers.** Disposable jammers are dropped in a certain area where they operate for various periods of time, jamming the electronic communications systems located in their vicinity. This type of jammer may be transported by aircraft, missiles, or artillery.

**m. Monopulse Deception.** If the input of the antenna is acted upon by signals of two coherent sources, it is possible in principle to create such a resultant signal by which the equisignal direction of a direction finder is oriented to a point located beyond the limits of the base.

# Appendix D

## Electronic Deception

### 1. General

This appendix is an introduction to electronic deception. It contains information useful when considering or countering electronic deception. For further information on military deception, see FMFM 7-13, *Military Deception*.

**a.** Electronic deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. (Quoted from the definition of electronic warfare, Joint Pub 1-02.)

**b.** Electronic deception is part of both electronic warfare and military deception. Normally, an electronic deception is conducted as part of a larger deception. Among the types of electronic deception are:

**(1) Manipulative Electronic Deception (MED).**

Actions to eliminate revealing, or convey misleading, telltale indicators that may be used by hostile forces.

**(2) Simulative Electronic Deception (SED).**

Actions to represent friendly, notional, or actual capabilities to mislead hostile forces.

**(3) Imitative Electronic Deception (IED).** The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.

**c.** Although electronic deception is usually thought of in terms of communications, electronic

deception is also conducted using noncommunication emissions.

### 2. Manipulative Electronic Deception

MED uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit is going to attack when it actually is going to withdraw, the unit might transmit notional (false) fire support plans and requests for ammunition.

MED can be used to cause the enemy to splinter his intelligence and electronic warfare efforts to the point that they lose their effectiveness. It can be used to cause the enemy to misdirect his ESM and ECM assets and, therefore, cause fewer problems with our communications. Used in these ways, MED is an ECCM technique.

The intelligence, artillery and air defense, and aviation elements are the primary users of noncommunication emitters. Each of these may be required to participate in MED.

### 3. Simulative Electronic Deception

SED uses communication and noncommunication signals to mislead hostile forces as to our units and/or the capabilities of our units. There are three types of simulations:

**a. Unit Simulation.** The use of actual equipment or specially designed simulators to indicate that a unit is in a certain location during a specified period.

**b. System Simulation.** The use of systems that give off emissions peculiar to a particular organization. A countermortar/counterbattery radar is peculiar to an artillery unit; therefore, by turning on that type radar, you can indicate the probable existence of an artillery unit.

**c. Activity Simulation.** The operation of non-communication emitters to imply a type or change of activity by a unit. For example, placing surveillance radars in a typical defensive array when, in fact, the intention is an attack.

#### 4. Imitative Electronic Deception

**a.** In IED, the enemy's electromagnetic emissions are imitated to mislead the enemy. Examples include entering enemy communications nets by using his call signs and radio procedures, and then giving enemy commanders instructions to make him do something to our advantage. Targets for IED include any enemy receiver and range from cryptographic systems to very simple, plain-language tactical nets. IED can cause a unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts are intended to cause decisions based on false information that appears to the enemy to have come from his own side.

**b.** Properly used, IED can be decisive on the battlefield. However, to be effective, IED requires electronic equipment capable of convincingly duplicating the functions of enemy equipment. IED can be done with any transmitter that (1) is compatible with the intended victim station equipment and (2) has sufficient power to transmit to the intended victim station. If available, however, captured enemy equipment should be used to ensure that the technical characteristics of signals are authentic. A proficient linguistic capability is required if voice transmissions are used. An operator capable of imitating the transmitting style of the enemy manual Morse operator is required when continuous wave is used. Unfortunately, the enemy is probably more skilled in communication deception than we are. His knowledge of English is extensive. He has been aided by our poor transmission security (TRANSEC) practices.

**c.** IED is usually less disruptive to the user's own communications than brute force jamming.

**d.** Examples of communications IED are:

"T4B9 this is L7N4, what is your location? Over."

"Cease fire, cease fire, there are friendlies in the area."

"Fire mission, 40 enemy troops in the open at coordinate HF...."

"M402 this is P4S3, radio silence is lifted."

"S806 this is Y5V4, proceed to hill 507 and await further orders."

**e.** The most effective deterrent to communications IED is proper use of codes and cipher systems. If these are not available or practical, then frequent, random changes of call signs and frequencies are the next best measures. The most effective countermeasure is authentication. Use designated authentication codes.

**f.** Imitative communication deception can be beaten. An alert operator can spot and counter IED. The enemy of course realizes that he will be more successful when battlefield fatigue begins to grow. That is when the supervisors need to increase their vigilance and make sure that operators do not get sloppy in their procedures. Authenticate at the slightest hint of IED. It may even be necessary to authenticate every transmission. Keep your operators alert and keep training them. All that is required for training against communications IED is the CEOI and compatible equipment.

**g.** Fortunately, those same conditions which cause problems for friendly communications and non-communications can also cause problems for the enemy. As his alertness decreases due to fatigue, it is easier to manipulate his thinking. Placing the IED plan into action at the correct time may help the commander win the battle.

**h.** IED will most likely succeed when enemy TRANSEC measures are unsophisticated or electronic equipment operators are lax and undisciplined. Imitative deception aimed at higher echelons is difficult because of the use of sophisticated cryptographic systems.

## 5. Electronic Deception Planning

**a.** Electronic deception planning determines how to use electromagnetic equipment to mislead the enemy and cause him to do something to our advantage (the deception objective).

**b.** Each piece of electronic and associated equipment has its own electronic signatures. These signatures are exploited in deception. An electronic signature may be identified by:

(1) Equipment characteristics, such as frequency, type of modulation, and power output.

(2) Employment of equipment, such as type of communications net; relative geographic positions; and correlations between communication and noncommunication equipment normally operating in the same unit or in the same geographic location.

(3) Operating procedures, such as schedules, traffic volume, patterns, distribution of messages within a single net, types of cryptology systems employed, and schedules for changes in call signs, frequencies, or other operating practices.

**c.** Deceptions are usually planned and supervised by the G-3/S-3. The CEO and EWO are usually responsible to the G-3/S-3 for the electronic deception plan. All of these personnel work with the G-2/S-2 to determine the electronic activities most likely to be intercepted by enemy SIGINT.

**d.** Careful integration of electronic deception with visual, sonic, and olfactory actions is critical. What the enemy detects electronically must agree with what he has seen, while others are simulated. Because of the reliance placed on electromagnetic radiation for communications, surveillance, navigation, etc., this aspect of deception requires close attention. Although electronic deception can be the sole act of a deception, its usefulness in that manner is usually short-lived.

**e.** The enemy's success depends on his knowledge of your emitters. Success in manipulative and simulative deceptions depends on knowing how

your emitters appear to the enemy. A profile (data base) of a command's communication and noncommunication emitters should be kept. This is to determine how best to electronically portray a desired portion of that command. When planning manipulative and simulative electronic deception, it is usually necessary to consider all the command's electromagnetic emitters. And it is necessary to consider what is occurring and what should occur with all electromagnetic emitters in the unit's area.

**f.** Similarly when planning an electronic deception, consider all unit electronic activities—those in support of ongoing activities as well as those that will support the deception operation. All must be integrated and mutually noninterfering. Close control and coordination will be necessary, especially during MED. Planning is done to avoid confusing friendly operators with information broadcast over friendly nets or with unique returns on noncommunication equipment.

**g.** Time is critical. Given sufficient time, the enemy can discover even the most complex electronic deception. A deception intended to deceive the enemy for two or three days, must include a well-coordinated electronic deception that covers all electronic emitters. In a deception for only a short period just before an attack, the electronic deception plan can be relatively simple.

**h.** Enemy capabilities are critical. If the enemy can not detect your electronic emitters, the electronic deception plan will probably be a waste of time.

**i.** MED and SED can be performed by any commander so long as he uses only equipment under his control. IED can only be done with permission of the appropriate commander. Within a MAGTF, this is usually the MAGTF commander. (Only skilled EW linguists tasked through the MAGTF headquarters will conduct ICD.) This is because IED can jeopardize the SIGINT effort. IED, if recognized by the enemy, will provide data concerning the friendly intercept effort. Thus, the enemy may be expected to improve his communications security and procedures to reduce the effectiveness of friendly SIGINT efforts. (**Warning:** Even though a commander has the capability to conduct MED and SED, he still must

coordinate such deceptions with higher, adjacent, support, and other appropriate headquarters. Among the calamities that can result from a failure to properly coordinate MED and SED is the deceiving of friendly forces.)

**j. False Emanation**

- (1) Must be on signals strong enough to reach the enemy.
- (2) Must be on a frequency the enemy can intercept.
- (3) Must be in a modulation the enemy can intercept.

**k. Electronic Deception Techniques**

- (1) Leave a significant sample of regimental or battalion headquarter’s communications in place while the headquarters moves to another location.

- (2) Broadcast false information with the intention of having the enemy receive the message and commit his forces into an area of our choosing.
- (3) Broadcast false unit strengths, dispositions, or locations to confuse the enemy intelligence analysts.
- (4) Exchange operators among units or overload one unit with operators whose characteristics are probably known to the enemy.
- (5) Place multichannel communications in a battalion area to show a larger size force.
- (6) Pad traffic on secure links to deceptively show a buildup for an attack. This technique applies to both voice and message traffic when encrypted.
- (7) Use call signs and frequencies in such a manner as to lead enemy analysts to incorrect net structures.

# Appendix E

## Communication ECCM Training

Effective MIJI, TRANSEC, and ECCM training can only be accomplished by using a live environment that includes active ECM (i.e., jamming and electronic deception). A unit can provide ECM (for training only) by establishing ECM teams manned by S-3 or CEO personnel, and use the unit's own communications equipment (e.g., MRC-110, PRC 77). The EWO employment of these ECM teams is strictly limited to the units daily frequencies and the normal maximum power output for the equipment that is used.

### 1. Jamming

The unit EWO must ensure that all jamming is done from locations beyond the FEBA. This procedure is realistic and allows such ECCM techniques as terrain masking of antennas to be effective. (In some past training attempts jammers have been located in unrealistic positions which rendered many ECCM techniques useless, thus teaching negative lessons.)

Jamming signals can be simulated with the units own equipment in a variety of methods, such as —

- Key the handset and blow into it.
- Record static or babbled voice on a cassette, and play it back into a keyed handset.
- Use a signal generator TIX (MD-492, SG-886/U) to supply the jamming signal. (These signal generators can be obtained through the supply system, or they can be temporarily loaned from the radio battalions.)

These jamming signals will be effective if the transmitter has sufficient power.

### 2. Imitative Communication Deception

The EWO should also direct the ECM team as to the type and number of ICD instructions they

may insert into the unit's nets. These instructions can be used to force communicators to authenticate, and maintain a high state of TRANSEC awareness. Concurrently with the use of ICD, the ECM team can also monitor the units nets for TRANSEC violations (compromises of security).

### 3. MIJI

The unit EWO should direct the ECM teams to maintain exact records of each jamming and ICD event. These records should be used to evaluate the effectiveness and accuracy of the unit's MIJI reporting procedures. MIJI reports provide valuable intelligence to the staff and should be formatted and forwarded in accordance with unit SOP. In order of importance, the uses for MIJI reports are —

- The Joint Electronic Warfare Center.
- The G-2, EWO, and CEO will use them to analyze enemy ECM tactics, then design/implement suitable ECCM.
- The reports will be used to key Marine direction finding units, which can obtain approximate locations of enemy jammers (DF cannot locate emitters with sufficient accuracy for indirect fire weapons).
- The reports are used by the CEO to isolate and eliminate interference.

# Appendix F

## Electronic Warfare Appendix Format

The electronic warfare appendix in operations orders and plans is normally APPENDIX 3 (Electronic Warfare) to ANNEX C (Operations). The format for this appendix is provided below.

### CLASSIFICATION

Copy No. \_\_\_\_ of \_\_\_\_ copies  
Issuing headquarters  
Place of issue  
Date/Time group  
Message reference number

APPENDIX 3 (Electronic Warfare) to ANNEX C (Operations) to Operation Order \_\_\_\_

Ref:

Time Zone:

#### 1. ( ) SITUATION

- a. ( ) Enemy. (Refer to Annex B [Intelligence] for an estimate of the capabilities, limitations, and vulnerabilities of enemy communications, radar, and EW systems, including the enemy's ability to interfere with the accomplishment of the EW mission of the unit issuing the plan or order.)
- b. ( ) Friendly. (Provide a summary of friendly EW facilities, resources, and organizations which may affect EW operations.)
- c. ( ) Assumptions. (State any assumptions on which EW operations are based.)

#### 2. ( ) MISSION

(State the mission to be accomplished by EW operations in support of the overall mission.)

#### 3. ( ) EXECUTION

- a. ( ) Concept of Operations. (Summarize the scope of EW operations and the methods and resources to be employed.)

(Page number)

CLASSIFICATION

CLASSIFICATION

- b.

( )

Tasks.

(In separate numbered subparagraphs, assign EW tasks and responsibilities to each appropriate unit.)
- c.

( )

Coordinating Instructions.

(Include instructions applicable to two or more subordinate units.)
4.

( )

GUIDING PRINCIPLES

(State or refer to policies, doctrine, and procedures which provide guidance to be followed in the execution of the plan or order. Describe any EW constraints which apply to the operation.)
5.

( )

SPECIAL MEASURES

(Provide guidance on the employment of each activity, special measure, or procedure which is to be used.)
6.

( )

ADMINISTRATION AND LOGISTICS

(Refer to Annex P [Combat Service Support]. Provide a statement of the administrative and logistic requirements for electronic warfare. Include instructions for special reporting.)

Signature

Name

Rank and Service

Title

(Page number)

CLASSIFICATION

# Appendix G

## Frequency Band Designations

### 1. Current Frequency Designations

Band	Frequency Range
A	0 - 250 MHz
B	250 - 500 MHz
C	500 - 1,000 MHz
D	1.0 - 2.0 GHz
E	2.0 - 3.0 GHz
F	3.0 - 4.0 GHz
G	4.0 - 6.0 GHz
H	6.0 - 8.0 GHz
I	8.0 - 10.0 GHz
J	10.0 - 20.0 GHz
K	20.0 - 40.0 GHz
L	40.0 - 60.0 GHz
M	60.0 - 100.0 GHz

**NOTE:** Each frequency band is divided into ten equal subbands, channels 1-10. To designate a specific frequency, use the band channel base plus frequency in Megahertz above the base. For example: 3,315 MHz = F4 plus 15.

### 2. International Radio Designations

Band	Frequency Range
Extra Low Frequency (ELF)	0 - 3 KHz
Very Low Frequency (VLF)	3 - 30 KHz
Low Frequency (LF)	30 - 300 KHz
Medium Frequency (MF)	300 - 3,000 KHz
High Frequency (HF)	3 - 30 MHz
Very High Frequency (VHF)	30 - 300 MHz
Ultra High Frequency (UHF)	300 - 3,000 MHz
Super High Frequency (SHF)	3 - 30 GHz
Extra High Frequency (EHF)	30 - 300 GHz

## Appendix H

## Glossary

## Section I. Acronyms

ACE .....	aviation combat element	ELSEC .....	electronics security
ADCON .....	administrative control	EMCON .....	emission control
AOA .....	amphibious objective area	EMI .....	electromagnetic interference
AOIC .....	assistant officer in charge	EMSEC .....	emissions security
ASM .....	air-to-surface missile	EOB .....	electronic order of battle
ATF .....	amphibious task force	ERIM .....	electronic reconnaissance intercept message
C <sup>3</sup> .....	command, control, and communications	ERIR .....	electronic reconnaissance intercept report
C <sup>3</sup> CM ...	command, control, and communications countermeasures	ERMAR .....	electronic reconnaissance mission analysis report
CATF .....	commander, amphibious task force	ESM .....	electronic warfare support measures
CE .....	command element	EW .....	electronic warfare
CEO .....	communications-electronics officer	EWO .....	electronic warfare officer
CEOI .....	communications-electronics operating instruction	FEBA .....	forward edge of the battle area
CLF .....	commander, landing force	FMFM .....	Fleet Marine Force manual
COB .....	communication order of battle	FSSG .....	force service support group
COC .....	combat operations center	GCE .....	ground combat element
COMINT .....	communications intelligence	GCI .....	ground control intercept
COMSEC .....	communications security	GS .....	general support
CP .....	command post	IAC .....	intelligence analysis center
CSSE .....	combat service support element	ICD .....	imitative communication deception
CW .....	continuous wave	IED .....	imitative electronic deception
DF .....	direction finding	JEWC .....	joint electronic warfare center
DOD .....	Department of Defense	JINTACCS .....	joint interoperability of tactical command and control systems
DST .....	direct support team	JSR .....	jamming-to-signal ratio
DSU .....	direct support unit	LF .....	landing force
ECCM .....	electronic counter-countermeasures		
ECM .....	electronic countermeasures		
EEl .....	essential elements of information		
ELINT .....	electronic intelligence		

MAGIS ...	Marine Air-Ground intelligence system	SAM .....	surface-to-air missile
MAGTF .....	Marine Air-Ground Task Force	SED .....	simulative electronic deception
MEB .....	Marine Expeditionary Brigade	S/EWCC.....	signals intelligence/electronic warfare communication center
MED .....	manipulative electronic deception	SI .....	special intelligence
MEF .....	Marine Expeditionary Force	SIGINT .....	signals intelligence
MEU .....	Marine Expeditionary Unit	SIGINT/EW .....	signals intelligence/electronic warfare
MIJI.....	meaconing, intrusion, jamming, and interference	SIGSEC.....	signal security
MRE .....	meal-ready-to-eat	SOP .....	standing operating procedure
MRL .....	multiple rocket launcher	SRIG .....	surveillance, reconnaissance, and intelligence group
NSA.....	National Security Agency	SSM .....	surface-to-surface missile
OCA .....	operation control and analysis	SYSCON.....	systems control
OCAC.....	operation control and analysis center	TEAM .....	tactical EA-6B mission planning system
OIC .....	officer in charge	TELINT .....	telemetry intelligence
OIR.....	other intelligence requirements	TERPES .....	Tactical Electronic Reconnaissance Processing and Evaluation System
OP .....	observation post	TRANSEC .....	transmission security
OPCON .....	operational control	VMAQ.....	Marine tactical electronic warfare squadron
OPREP .....	operations report	WARM .....	wartime reserve mode
OPSEC .....	operations security		
OTH .....	over-the-horizon		
POL .....	petroleum, oil, and lubricants		
RDF .....	radio direction finding		
REC .....	radioelectronic combat		
RRT .....	radio reconnaissance team		

## Section II. Definitions

### A

**active jamming** — Electronic jamming that uses original signals.

**administrative control** — Direction or exercise of authority over subordinate or other organizations in respect to administrative matters such as personnel management, supply, services, and other matters not included in the operational missions of the subordinate or other organizations. (Joint Pub 1-02)

**assign** — 1. To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel. 2. To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (Joint Pub 1-02)

**attach** — 1. To place units or personnel in an organization where such placement is relatively temporary. Subject to limitations imposed in the attachment order, the commander of the formation, unit, or organization receiving the attachment will exercise the same degree of command and control thereover as he does over the units and persons organic to his command. However, the responsibility for transfer and promotion of personnel will normally be retained by the parent formation, unit, or organization. 2. To detail individuals to specific functions where such functions are secondary or relatively temporary; e.g., attach for quarters and rations, attach for flying duty. (Joint Pub 1-02)

### B

**basic requirements** — Items of information regarding the enemy and his environment. These state the requirements for basic intelligence.

### C

**collection agency** — Any individual, organization, or unit that has access to sources of information and

the capability of collecting information from them. (Joint Pub 1-02)

**combat information** — Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (Joint Pub 1-02)

**combat intelligence** — That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Joint Pub 1-02)

**command** — The authority that a commander in the military Service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. (Joint Pub 1-02) (Part one of three-part definition.)

**control** — 1. Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (Joint Pub 1-02) (Part one of four-part definition.)

**coordination** — (1) The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as: emergency defense measures; area intelligence and security; area public and labor relations; common supply; utilities; public works; leases and space assignments; transportation; prescription of area uniform regulations; sanitation and health measures; area maintenance of standards in discipline, legal assistance and welfare; and other situations in which coordination is considered necessary. (Marine Corps Manual) (2) The act of bringing things into a common action, movement, or condition in order to achieve a specific goal.

**D**

**direct support** — A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance. (Joint Pub 1-02)

**E**

**electromagnetic interference** — Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. Also called **EMI**. (Joint Pub 1-02)

**electronic warfare** — Military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of electromagnetic spectrum. Also called **EW**. There are three divisions with electronic warfare:

**a. electronic countermeasures** — That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Also called **ECM**. Electronic countermeasures include:

(1) **electronic jamming** — The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment, or systems.

(2) **electronic deception** — The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. Among the types of electronic deception are: (a) **manipulative electronic deception** — Actions to eliminate revealing, or convey misleading, telltale indicators that may be used by hostile forces. (b) **simulative electronic deception** — Actions to represent friendly notional or actual capabilities to mislead hostile forces.

(c) **imitative electronic deception** — The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.

**b. electronic counter-countermeasures** — That division of electronic warfare involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of electronic warfare. Also called **ECCM**.

**c. electronic warfare support measures** — That division of electronic warfare involving actions taken under direct control of an operational commander to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support measures (**ESM**) provide a source of information required for immediate decisions involving electronic countermeasures (**ECM**), electronic counter-countermeasures (**ECCM**), avoidance, targeting, and other tactical employment of forces. Electronic warfare support measures data can be used to produce signals intelligence (**SIGINT**), both communications intelligence (**COMINT**) and electronics intelligence (**ELINT**). Also called **ESM**.

**emission control** — The selective controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security (**OPSEC**), detection by enemy sensors; to minimize mutual interference among friendly systems; and/or to execute a military deception plan. Also called **EMCON**. (Joint Pub 1-02)

**essential elements of information** — The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. (Joint Pub 1-02)

**G**

**general support** — That support which is given to the supported force as a whole and not to any particular subdivision thereof. (Joint Pub 1-02)

**guarded frequencies** — Frequencies in use by the enemy and of use as a source of intelligence to the friendly force. Jamming activities on these frequencies are normally controlled by intelligence staffs.

## I

**information** — In intelligence usage, unevaluated material of every description which may be used in the production of intelligence. (Joint Pub 1-02) (Part one of two-part definition.)

**intelligence** — The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas. (Joint Pub 1-02)

**intelligence requirement** — Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (Joint Pub 1-02)

## O

**obvious jamming** — Jamming so conducted that the enemy can easily detect it.

**operational control** — Transferable command authority which may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in Combatant Command (command authority) and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations; normally this authority is exercised through the Service component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called **OPCON**. (Joint Pub 1-02)

**organic** — Assigned to and forming an essential part of a military organization. Organic parts of a unit are

those listed in its table of organization for the Army, Air Force, and Marine Corps and are assigned to the administrative organizations of the operating forces for the Navy. (Joint Pub 1-02)

**other intelligence requirements** — Items of information desired regarding the enemy and his environment.

## P

**passive jamming** — Electronic jamming that repeats signals.

**preventive ECCM** — Those electronic counter-countermeasures taken during training, planning, and the establishment of communications systems.

**protected frequencies** — Frequencies allocated for operational use by the friendly force and on which jamming must be minimized.

## R

**remedial ECCM** — The electronic counter-countermeasures taken when confronted with electronic countermeasures.

## S

**signals intelligence/electronic warfare coordination center** — A Marine Corps staff agency where signals intelligence and electronic warfare operations are coordinated.

**source** — A person, thing, or activity from which intelligence information is obtained. (Joint Pub 1-02) (Part one of three-part definition.)

**subtle jamming** — Electronic jamming that is not easily detected.

## T

**TABOO frequencies** — Frequencies of such importance that they must never be jammed. They may be critical to friendly force activities (e.g., command and control) or in use by the enemy and of exceptional importance for intelligence gathering.

**tasking authority**— The authority to direct an electronic warfare unit or element to conduct signals intelligence, electronic warfare support measures (ESM), or electronic countermeasures (ECM) activities.

**technical direction**— The performance of a specialized or professional service, or the exercise of professional guidance or direction through the establishment of policies and procedures in technical matters. Technical direction may include—

- (1) Establishing standards or procedures for performing a technical function.
- (2) Providing professionally trained and qualified personnel to perform a technical function.
- (3) Providing professional advice, guidance, or assistance.
- (4) Performing a technical function as a service to the command. (Marine Corps Manual)

# Appendix I

## References

### 1. Joint Publication

Joint Pub 3-51      Command, Control, and Electronic Warfare in Joint Military Operations (S)

### 2. Fleet Marine Force Manuals

FMFM 3-3E	Radio Operator's Handbook
FMFM 3-3F	Guide to Electromagnetic Interference Control
FMFM 5-6	Air Reconnaissance
FMFM 7-13	Military Deception

### 3. U.S. Naval Warfare Publications

NWP 10-1-40	Electronic Warfare Coordination (S)
NWP 10-1-41	Navy Operational Deception and Counterdeception (SNF)
NWP 12-6	Tactical Electronic Warfare Planning Guide (S)
NWP 12-6.1	Threat Emitter Evaluation Guide (S)
NWP 12-6.2	Neutral/Friendly Emitter Guide (S)
NWP 55-7-1	Air Reconnaissance and Surveillance Manual

### 4. U.S. Army Field Manuals

FM 21-31	Topographic Symbols
FM 24-18	Tactical Single-Channel Radio Communications Techniques
FM 24-33	Communications Techniques: Electronic Counter-Countermeasures
FM 34-1	Intelligence and Electronic Warfare Operations
FM 34-37	Echelons Above Corps Intelligence and Electronic Warfare Operations
FM 34-40	Electronic Warfare Operations
FM 34-60	Counterintelligence
FM 34-86	Direction Finding Operations
FM 34-88	Morse Code Intercept Operations

5. Marine Corps Orders

MCO 3430.1	Performing ECM in the U.S. and Canada
MCO 3430.2	Electronic Warfare Policy
MCO 3430.3	RPT Beaconing, Intrusion, Jamming, and Interference of Electromagnetic Sys Rcs

6. Allied Publication

ATP-44	Electronic Warfare (EW) in Air Operations
--------	---

7. Other Publications

JDA 1-87	JEWC DOD Responses to Hostile Wartime Reserve Modes (WARM) (U)
JDD 1-83	JCS/JEWC Joint Electronic Warfare Manual
JDD 1-86	JEWC Joint Task Force EW Planning Manual (C)
JDD 1-87	JEWC Joint Task Force C <sup>3</sup> CM Planning Manual (S)
JDD 1-88	JEWC C <sup>3</sup> /C <sup>3</sup> CM Handbook (S)
JDX 1-84	Vol. II, JEWC Joint Exercise Manual for Employment of EW, EW and C <sup>3</sup> CM Lessons Learned (S)
JDX 1-89	JEWC Joint Exercise Manual for Employment of EW Planning and Execution
OPTEVFOR	Tactics Guide—EA-6B (S)
	Communications Jamming Handbook—JCGW-78-2 (S)
	Electronic Parameter Limits (EPL) List (S)
	Capabilities Handbook (S)

# Index

		Page
<b>A</b>		
Active jamming .....	2003a(3)(a)	2-3
Barrage .....	2003a(3)(a) <u>2</u>	2-4
Spot .....	2003a(3)(a) <u>1</u>	2-4
Sweep .....	2003a(3)(a) <u>3</u>	2-4
Airborne electronic warfare .....	2009	2-11
Capabilities .....	2009c	2-12
Characteristics .....	2009a	2-11
Limitations .....	2009d	2-12
Requirements .....	2009b	2-12
Authority of area commander .....	5003	5-3
Commanders and their staffs .....	2006	2-8
Delegation .....	2006c	2-9
Responsibility .....	2006a	2-8
<b>B</b>		
Basic requirements .....	2002d(5)(a)	2-3
<b>C</b>		
Combat information .....	2002c(4)	2-3
Combat intelligence .....	2002c(3)	2-3
Command .....	2007a	2-9
Components .....	2007a(1)	2-9
Administrative .....	2007a(1)(b)	2-9
Coordination .....	2007c	2-10
Operational .....	2007a(1)(a)	2-9
Technical direction .....	2007a(1)(d)	2-9
Relationships .....	5002a	5-1
ADCON .....	2007a(1)(b), 5002d(6)	2-9, 5-3
Assign .....	5002a(3)	5-1
Advantages/disadvantages .....	5002d(3)	5-2
Attach .....	5002a(4)	5-1
Advantages/disadvantages .....	5002d(4)	5-2
Command .....	2007a	2-9
Advantages/disadvantage .....	5002d(1)	5-2
OPCON .....	2007a(2)	2-9
Advantages/disadvantages .....	5002d(5)	5-2
Organic .....	5002a(2)	5-1
Advantages/disadvantages .....	5002d(2)	5-2

		Page
Communications .....	2005	2-8
ECCM training .....	App. E	E-1
Intelligence .....	1005a	1-3
Security .....	1006a	1-4
Control .....	2007b	2-10
Coordination .....	2007c	2-10
Cryptosecurity .....	1006a(1)	1-5
<b>D</b>		
Direct support .....	5002b(1)	5-1
Doctrine .....	1001a(1)	1-1
Duties of personnel .....	3006	3-3
Communications-electronics officer .....	3006e	3-4
Electronic warfare officer .....	3006d	3-4
Intelligence officer .....	3006a	3-3
Operations officer .....	3006c	3-4
Special intelligence officer .....	3006b	3-4
<b>E</b>		
Electromagnetic interferences .....	2003a(7)	2-6
Electronic counter-countermeasures .....	2004a(2), 2004	2-1, 2-7
Classification .....	2004d	2-8
Preventive ECCM .....	2004d(1)	2-8
Remedial ECCM .....	2004d(2)	2-8
Combat .....	2004b	2-8
Technical protection .....	2004a	2-8
Techniques .....	6001	6-1
Preventive ECCM .....	6002	6-1
Remedial ECCM .....	6003	6-3
Updating .....	2004c	2-8
Electronic countermeasures .....	2001a(1), 2003	2-1, 2-3
Electronic deception .....	2001a, 2003b,	2-1, 2-7,
Application .....	App. D	D-1
Electronic jamming .....	2003b(2)	2-7
2001a, 2003a,		2-1, 2-3,
Concentration .....	App. C	C-1
Control .....	2003a(4)	2-3
Effect .....	2003a(2)	2-3
Minimizing interference .....	2003a(1)	2-3
Modes .....	2003a(7)	2-6
Planning and employment .....	2003a(3)	2-3
Timing .....	2003a(6)	2-4
Electronic threat:	2003a(5)	2-4
Complimentary roles between RDF and ECM .....	10008	10-6
Between RDF and intercept .....	10007	10-5

		Page
Electronic threat (Continued)		
Concepts	10002	10-1
EW capabilities	10004	10-2
Barrage jamming	10004b(3)	10-2
Direction finding	10004b(2)	10-2
ELINT security	10004c(1)	10-2
Frequency diversity	10004c(2)	10-2
Intrusion	10004b(4)	10-2
Mobility	10004c(4)	10-2
Multiple and interchangeable guidance	10004c(3)	10-2
SIGINT interception	10004b(1)	10-2
Radioelectronic combat	10006	10-3
Conduct	10006d	10-4
Planning	10006c	10-4
Priorities	10006b	10-3
Radiomas kirova	10006f	10-5
Signals intelligence threat	10006e	10-5
Tactical reconnaissance	10005	10-2
Air reconnaissance	10005a	10-2
Electronic intercept and direction finding	10005b	10-3
Reaction time	10005b(3)	10-3
Electronic warfare	2001	2-1
Amphibious operations	9001	9-1
Assault	9001e	9-1
Embarkation	9001b	9-1
Movement	9001c	9-1
Planning	9001a, 9004	9-1, 9-3
Rehearsal	9001d	9-1
Responsibilities	9002	9-2
CATF	9002a	9-2
CLF	9002b	9-2
Tasks during planning	9003	9-3
Appendix format	App. F	F-1
Command and support relationships	5002	5-1
Coordination and control	2001d, 5001,	2-2, 5-1
	5005	5-4
Doctrine	2001	2-1
Employment of units with GCE	8001	8-1
Concepts of employment	8004	8-2
Direct support reporting chain	Fig. 8-3	8-4
General support reporting chain	Fig. 8-2	8-3
Employment considerations	8003	8-1
Support relationship	Fig. 8-1	8-2
Planning considerations	8002	8-1
Integration in operations	2001c	2-2

		Page
Electronic warfare (Continued)		
Officer .....	9005a	9-3
Planning .....	4001	4-1
ECM plans .....	4003	4-1
Format .....	Fig. 4-5	4-5
Planning tasking .....	Fig. 4-4	4-4
Report .....	Fig. 4-6	4-5
ESM plans .....	4002	4-1
Purpose .....	2001b	2-2
Reports .....	7001	7-1
Classifications .....	7003b	7-2
Distribution .....	7003c	7-2
Formats .....	7003d	7-2
MIJI .....	7002	7-1
TERPES-generated .....	7003	7-1
ERIM .....	7003a(1)	7-1
ERIR .....	7003a(2)	7-1
ERMAR .....	7003a(3)	7-1
JINTACCS .....	7003a(5)	7-2
OPREP-4 .....	7003a(4)	7-1
Responsibilities .....	2001e	2-2
Support measures .....	2002	2-2
ESM support to intelligence .....	2002b	2-2
Intelligence support .....	2002a	2-2
Various types of operations .....	2010	2-12
Advance to contact .....	2010d	2-13
Defensive .....	2010b	2-13
Delaying .....	2010c	2-13
Offensive .....	2010a	2-12
Withdrawal .....	2010e	2-13
Electronics intelligence .....	1005b	1-3
Security .....	1006c	1-4
Emission security .....	1006a(3)	1-4
Essential elements of information .....	2002c(5)	2-3

## F

Foreign instrumentation signals intelligence .....	1005e	1-3
Frequencies .....	2003a(7)(b)	2-6
Guarded frequencies .....	2003a(7)(b)2	2-6
Protected frequencies .....	2003a(7)(b)3	2-6
TABOO frequencies .....	2003a(7)(b)1	2-6
Frequency band designations .....	App. G	G-1

## G

General support .....	5002b(2)	5-2
Graphic formats and color coding .....	App. A	A-1

		Page
Ground electronic warfare .....	2008	2-10
Capabilities .....	2008c	2-11
Characteristics .....	2008a	2-10
Limitations .....	2008d	2-11
Requirements .....	2008b	2-10
<b>I</b>		
Imitative electronic deception .....	2004b	2-7
Information .....	2002c(2)	2-3
Intelligence .....	2002c(1)	2-2
Requirements .....	2002c(5)	2-3
<b>J</b>		
Jamming .....	2003a(6)(e)	2-5 – 2-6
Obvious .....	2003a(6)(e)1	2-5
Subtle .....	2003a(6)(e)2	2-6
Joint tactical electronic warfare request format .....	App. B	B-1
<b>M</b>		
MAGTF structure .....	1002	1-2
ACE .....	1002c	1-3
Command element .....	1002a	1-2
CSSE .....	1002d	1-3
GCE .....	1002b	1-2
Manipulative electronic deception .....	2001a	2-1
Marine tactical electronic warfare squadron .....	3003	3-1
<b>N</b>		
National level agencies .....	3005	3-2
Joint electronic warfare center .....	3005b	3-3
National Security Agency .....	3005a	3-2
<b>O</b>		
Other intelligence requirement .....	2002c(5)(c)	2-3
<b>P</b>		
Passive jamming .....	2003a(3)(b)	2-4
Chaff .....	2003a(3)(b)3	2-4
Reflectors .....	2003a(3)(b)4	2-4
Repeaters .....	2003a(3)(b)1	2-4
Transponders .....	2003a(3)(b)2	2-4

		Page
Physical security .....	1006a(4)	1-4
Preventive ECCM .....	6002	6-1
Execution .....	6002c	6-3
Planning .....	6002b	6-2
Combat information/intelligence .....	6002b(1)	6-2
EMCON .....	6002b(3)	6-3
System design .....	6002b(2)	6-2
Training .....	6002a	6-1
Procedure .....	1001a(4)	1-2
 <b>R</b>		
Radio battalion .....	3002	3-1
Detachment AOIC .....	9005c	9-3
Detachment OIC .....	9005b	9-3
Remedial ECCM .....	6003	6-3
 <b>S</b>		
Signal security .....	1006	1-3
Signals intelligence .....	1005	1-3
Electronic warfare coordination center .....	3007	3-4
Simulative electronic deception .....	2001a	2-1
Source .....	2002c(7)	2-3
Standing operating procedures .....	1004	1-3
 <b>T</b>		
Tactics .....	1001a(2)	1-1
Tasking authority .....	5004	5-4
Tasking MAGTF assets .....	5006	5-4
Collection tasking .....	5006a	5-4
Electronic countermeasures tasking .....	5006b	5-5
Techniques .....	1001a(3)	1-1
Telemetry intelligence .....	1005c	1-3
TERPES .....	3003c	3-2
AN/TSQ-90C .....	3003c(1)	3-2
Electronic order of battle .....	3003c(2)	3-2
MAGIS .....	3003c(3)	3-2
Training .....	1003	1-3
Transmission security .....	1006a(2)	1-4